Intermec

User's Manual

IF5 Fixed Reader

Intermec Technologies Corporation

Worldwide Headquarters
6001 36th Ave.W.
Everett, WA 98203
U.S.A.

www.intermec.com

The information contained herein is proprietary and is provided solely for the purpose of allowing customers to operate and service Intermec-manufactured equipment and is not to be released, reproduced, or used for any other purpose without written permission of Intermec.

Information and specifications contained in this document are subject to change without prior noticed and do not represent a commitment on the part of Intermec Technologies Corporation.

© 2004-2006 by Intermec Technologies Corporation. All rights reserved.

The word Intermec, the Intermec logo, Norand, ArciTech, Beverage Routebook, CrossBar, dcBrowser, Duratherm, EasyADC, EasyCoder, EasySet, Fingerprint, INCA (under license), i-gistics, Intellitag, Intellitag Gen2, JANUS, LabelShop, MobileLAN, Picolink, Ready-to-Work, RoutePower, Saber, ScanPlus, ShopScan, Smart Mobile Computing, SmartSystems, TE 2000, Trakker Antares, and Vista Powered are either trademarks or registered trademarks of Intermec Technologies Corporation.

Throughout this manual, trademarked names may be used. Rather than put a trademark (™ or ®) symbol in every occurrence of a trademarked name, we state that we are using the names only in an editorial fashion, and to the benefit of the trademark owner, with no intention of infringement.

There are U.S. and foreign patents pending.

Wi-Fi is a registered certification mark of the Wi-Fi Alliance.

Microsoft, Windows, and the Windows logo are registered trademarks of Microsoft Corporation in the United States and/or other countries.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (www.openssl.org).

This product includes cryptographic software written by Eric Young (EAY@cryptsoft.com).

Document Change Record

This page records changes to this document. The document was originally released as Revision 001.

Revision	Date	Description of Change
002	11/2005	Added information supporting Release 2.0 firmware: • Configuring the IF5 using the web browser interface • Guidelines for developing and testing RFID applications • Configuring the SAP device controller RFID edgeware • Guidelines for using the IF5 general purpose input/output (GPIO) interfaces
003	2/2006	Added information supporting Release 2.01 and 2.02 firmware: • Descriptions of the IBM WRDI option and WEDM settings • Support for EPCglobal Class 1 Gen 2 RFID tags
004	11/2006	Added information supporting Release 2.20 firmware: • Minor changes to the IF5 web browser interface • Descriptions of data processors for the SAP device controller RFID edgeware • Description of the J2SE option • Support for dense reader mode and Listen Before Talk feature

Contents

Before You Begin. xiii
Safety Information xiii
Global Services and Support xiii
Warranty Information xiii
Web Support xiv
Telephone Support xiv
Who Should Read This Manual xv
Related Documents xv
Patent Information xvi

1 Getting Started 1

Overview of the IF5 2

What's New? 2

Unpacking the IF5 3

Learning About the IF5 4
Understanding the Front Panel Ports 4
Understanding the LEDs 6
About the Intermec Ready-To-Work Indicator 7
Understanding the Rear Panel Ports 8

How the IF5 Fits in Your Network 9

Configuring the IF5 (Setting the IP Address) 10
Using a Communications Program 10
Configuring the IF5 for an Ethernet Connection 13
Configuring the IF5 for a Wireless Network 15
Using the Web Browser Interface 19

Saving Configuration Changes 22

Installing the IF5 24
Choosing a Mounting Location 24
Connecting the IF5 to Your Network 25
Positioning 802.11g Antennas 26

Setting the Date and Time 27

Using the IF5 Securely 28

2 Configuring Network Settings 29

Configuring Settings for Your Network 30

Configuring Ethernet Settings 30
Enabling IPv6 33

Configuring Network Services 34
Configuring SNTP Client Settings 36

Configuring the 802.11g Radio 37
Configuring Advanced Parameters 39

Configuring Security 41
Controlling Access to IF5 Menus 42
Controlling Developer Access 44
Setting Up Logins 45
Configuring the IF5 to Use a Password Server 46
Changing the Default Login 48
Configuring Static WEP Security 50
Configuring Dynamic WEP/802.1x Security 52
Configuring WPA-PSK Security 54
Configuring WPA-802.1x Security 55
Configuring WPA2-PSK Security 57
Configuring WPA2-802.1x Security 58
Configuring 802.1x Client Settings 60

About Certificates 61
Viewing Certificates 61
Installing and Uninstalling Certificates 62
Rejecting Expired Certificates 64

3 Developing and Using RFID Applications 65

RFID Applications and the IF5 66
About the IBM WRDI Option 66
About the J2SE Option 67

Creating RFID Applications for the IF5 67
Using the RFID Resource Kit 67
IF5 Java Support 68
Executing Java Applications 68
Java Support for Microsoft SQL Servers 69

IF5 JavaScript Support 70

Running Applications at Boot Time 70
Handling Command Line Arguments at Boot Time 71

About IF5 Edgeware 71

About the IF5 RFID Architecture 73

Configuring RFID Settings 74
About RFID Module Settings 75
Supported Tag Type (ISO) 75
Supported Tag Type (Gen 1) 75
Supported Tag Type (Gen 2) 75
Dense Reader Mode 75
LBT Channel 76
LBT Scan Enable 76
Field Separator 76
ID Report 76
No Tag Report 76
Timeout Configuration Mode 76
ID Tries 77
ID Timeout 77
Antenna Tries 77
Antenna Timeout 77
Read Tries 78
Write Tries 78
Init Tries 78
Lock Tries 78
Select Tries 78
Unselect Tries 78
Initial Queue 79
Field Strength 79
Session 79
Enable Antenna Port *n* *79*

Configuring the Data Collection Engine 80
Viewing the DCE Events Log 82
Viewing DCE Statistics 83

Using the Diagnostics Tool 84
Displaying Tags 85
Testing the GPIO Interfaces 86
Using the BRI Window 87
Measuring Tag Read Performance 88
About the Performance Test 90

Using the JavaScript Tool 90
Using the JavaScript Workbench 91
Configuring a JavaScript File to Auto-Run at Boot Time 92
Editing Remote Startup Files 94

Configuring WEDM Settings 95

4 Managing, Troubleshooting, and Upgrading the IF5 . . . 97

Managing the IF5 98

Using Simple Network Management Protocol (SNMP) 98

Using Wavelink Avalanche 101

Using the Intermec SmartSystems Console 103
Configuring the IF5 with Intermec Settings 103

Importing and Exporting Files 104
Using the Web Browser to Import and Export Files 104
Browsing the IF5 and Importing Files to Your PC 104
Importing Files to the IF5 106
Using the FTP Server to Import and Export Files 108

Maintaining the IF5 110
Viewing Connections 110
Viewing Access Point Neighbors 111
Viewing Port Statistics 113
Viewing the Events Log 113
Viewing the About This IF5 RFID Reader Screen 114
Using the LEDs to Locate the IF5 115
Viewing the IF5 Configuration Summary 116
Restoring the IF5 to the Default Configuration 118

Troubleshooting the IF5 119
Problems While Working With RFID 119
Problems With Connectivity 120
Problems With Copying Files 122

Calling Intermec Product Support 122

Upgrading Firmware 123

5 Using the IF5 GPIO Interfaces 125

About the GPIO Interfaces 126

Accessing the Interfaces 126

Using the Input Interfaces 127
- IF5 Powered Input 127
- Isolated Input Interface 128
- Open Collector Input Interface 128

Using the Output Interfaces 129
- Switching the High Side Using IF5 Power 130
- Switching the Low Side Using IF5 Power 130
- Switching the High Side Using External Power 131
- Driving a DC Relay to Control an AC Load 131

Using the Power Interface 132

A Specifications 133

IF5 Specifications 134

802.11g Radio Specifications 135

RFID Specifications 136

Port Pin Assignments 137
- Control Port 137
- Serial Port 138
- Ethernet Port 138

B Configuring and Using the SAP Device Controller 139

Enabling the SAP Device Controller 140
- Running the Device Controller Manually 140
  - Opening a Telnet Session to the IF5 141
  - Starting and Stopping the Device Controller Manually 141
  - Reconfiguring the Device Controller Manually 141
- Stopping or Reconfiguring the Device Controller Over the Network 142

Using the Configuration File Generator 142

About the SAP-DC Configuration Files 143
Changing Settings in the Configuration Files 144
About the SDCConfiguration XML File 144
Controller ID 144
ReceiverList 145
Reader List 146
FieldMap 146
ExtensionCommandHandler 146
ProcessorChainList 146
About the RfidReader.properties File 148
Setting Parameters for Logging 151

Using the Data Processors 152
Data Processor Types 154
Standard Data Processors 156
CheckReader 156
DuplicateFilter 156
SimpleDuplicateFilter 156
EPCEnricher 156
EqualizeTimeStamp 157
EventTypeFilter 157
HierarchyBuilderSend 157
SimplePackSend 158
LowPassFilter 158
SelectedFieldEnricher 158
Send 158
TagBitsFilter 158
TimeFixedSizeAggregator 159
About Transformers 159
EPCPMLTransformer 159
MultiEPCPMLTransformer 159
PMLTransformer 159
PMLTransformer2 159
PMLTransformerAII4 159
ValidEPCPMLTransformer 159
About Data Processor Options 160
Options for All Processor Types 160
Options for Send Processors 160
Options for CheckReader 160
Options for EPCEnricher 161
Options for EventTypeFilter 161
Options for HierarchyBuilderSend 161
Options for SimplePackSend 161
Options for LowPassFilter 162
Options for SelectedFieldEnricher 162
Options for TagBitsFilter 163

Options for TimeFixedSizeAggregator 163

Index 165

Before You Begin

This section provides you with safety information, technical support information, and sources for additional product information.

Safety Information

Your safety is extremely important. Read and follow all cautions in this document before handling and operating Intermec equipment. Your equipment and data can be damaged if you do not follow the safety cautions.

This section explains how to identify and understand cautions and notes that are in this document.

A caution alerts you to an operating procedure, practice, condition, or statement that must be strictly observed to prevent equipment damage or destruction, or corruption or loss of data.

Note: Notes either provide extra information about a topic or contain special instructions for handling a particular condition or set of circumstances.

Global Services and Support

Warranty Information

To understand the warranty for your Intermec product, visit the Intermec web site at www.intermec.com and click **Service & Support**. The Intermec Global Sales & Service page appears. From the Service & Support menu, move your pointer over **Support**, and then click **Warranty**.

Disclaimer of warranties: The sample code included in this document is presented for reference only. The code does not necessarily represent complete, tested programs. The code is provided "as is with all faults." All warranties are expressly disclaimed, including the implied warranties of merchantability and fitness for a particular purpose.

Web Support

Visit the Intermec web site at www.intermec.com to download PDF versions of our current manuals. To order printed versions of the Intermec manuals, contact your local Intermec representative or distributor.

Visit the Intermec technical knowledge base (Knowledge Central) at intermec.custhelp.com to review technical information or to request technical support for your Intermec product.

Telephone Support

These services are available from Intermec Technologies Corporation.

Services	Description	In the USA and Canada call 1-800-755-5505 and choose this option
Order Intermec products	• Place an order. • Ask about an existing order.	1 and then choose 2
Order Intermec media	Order printer labels and ribbons.	1 and then choose 1
Order spare parts	Order spare parts.	1 or 2 and then choose 4
Product Support	Talk to technical support about your Intermec product.	2 and then choose 2.
Service	• Get a return authorization number for authorized service center repair. • Request an on-site repair technician.	2 and then choose 1

Outside the U.S.A. and Canada, contact your local Intermec representative. To search for your local representative, from the Intermec web site, click **Contact**.

Who Should Read This Manual

This user's manual is for the person who is responsible for installing, configuring, and maintaining the IF5 Fixed Reader.

This manual provides you with information about the features of the IF5, and how to install, configure, operate, maintain, and troubleshoot it.

Before you work with the IF5, you should be familiar with your network and general networking terms, such as IP address. You should also be familiar with your RFID system.

Related Documents

This table contains a list of related Intermec documents and their part numbers.

Document Title	Part Number
IF5 Fixed Reader Quick Start Guide	930-069-xxx
Basic Reader Interface Programmer's Reference Manual	937-000-xxx
Important IF5 Information!	074934
IM5 Compliance Insert	075231

The Intermec web site at www.intermec.com contains our documents (as PDF files) that you can download for free.

To download documents

1. Visit the Intermec web site at www.intermec.com.
2. Click **Service & Support** > **Manuals**.
3. In the **Select a Product** field, choose the product whose documentation you want to download.

To order printed versions of the Intermec manuals, contact your local Intermec representative or distributor.

Patent Information

Product is covered by one or more of the following patents:

4,739,328; 4,786,907; 4,864,158; 4,888,591; 4,910,794; 4,999,636; 5,030,807; 5,055,659; 5,070,536; 5,280,159; 5,295,154; 5,349,678; 5,394,436; 5,425,051; 5,428,636; 5,483,676; 5,504,485; 5,504,746; 5,521,601; 5,546,397; 5,550,547; 5,574,979; 5,592,512; 5,673,037; 5,680,633; 5,682,299; 5,696,903; 5,740,366; 5,763,867; 5,777,561; 5,790,536; 5,825,045; 5,828,318; 5,828,693; 5,844,893; 5,850,181; 5,850,187; 5,862,171; 5,940,771; 5,942,987; 5,960,344; 5,995,019; 6,078,251; 6,121,878; 6,122,329; 6,172,596; 6,195,053; 6,249,227; 6,280,544; 6,286,762; 6,286,763; 6,288,629; 6,360,208; 6,384,712; 6,404,325; 6,429,775; 6,486,769; 6,501,807; 6,525,648; 6,639,509; 6,645,327; 6,677,852; 6,768,414; 6,784,789; 6,816,063.

There may be other U.S. and foreign patents pending.

1 Getting Started

This chapter introduces the IF5 Fixed Reader, explains the ports and LEDs, and explains how the reader fits into your network. It contains these topics:

- Overview of the IF5
- What's New?
- Unpacking the IF5
- Learning About the IF5
- How the IF5 Fits in Your Network
- Configuring the IF5 (Setting the IP Address)
- Saving Configuration Changes
- Installing the IF5
- Setting the Date and Time
- Using the IF5 Securely

Overview of the IF5

The IF5 Fixed Reader is an RFID reader that provides wired or wireless connectivity between tag data and an enterprise system.

Note: The IF5 does not ship with RFID or radio antennas. For more information on these accessories, contact your Intermec sales representative.

What's New?

This manual supports Release 2.20 of the IF5, which includes these new features:

- RFID module support for Dense Reader Mode and Listen Before Talk.
- You can order the IF5 with the Java J2SE option. For more information, contact your Intermec sales representative.

Unpacking the IF5

When you unpack the IF5, save the box and shipping material in case you need to ship or store the IF5. The reader comes with a documentation packet that includes a quick start guide and radio safety compliance statements.

The IF5 with an IEEE 802.11g radio installed is Wi-Fi® certified for interoperability with other 802.11g and 802.11b wireless LAN devices.

The IF5 Fixed Reader uses an EPCglobal Gen 2-certified IM5 Module (86x MHz RFID frequency band).

950110126000000094

The IF5 Fixed Reader uses an EPCglobal Gen 2-certified IM5 Module (915 MHz RFID frequency band).

950110126000000100

Learning About the IF5

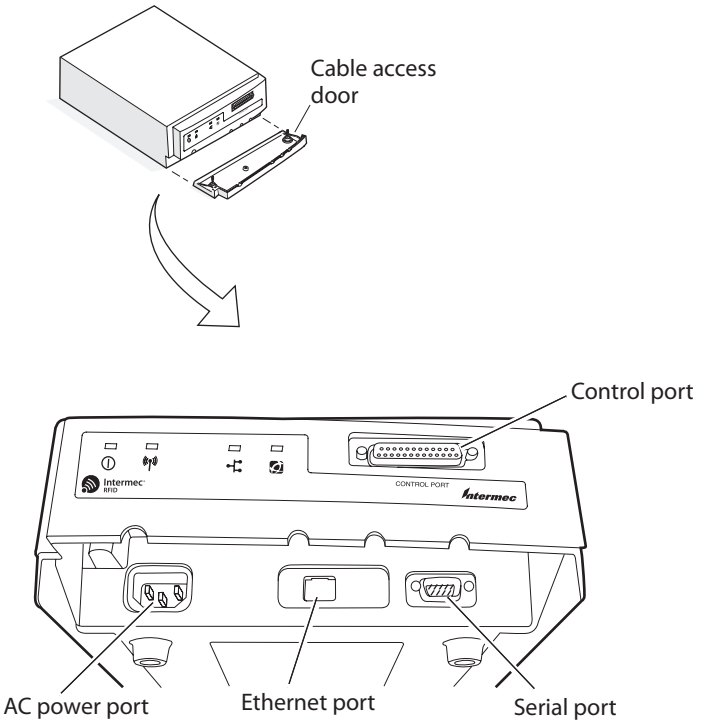
This section explains the ports and LEDs on the IF5.

Understanding the Front Panel Ports

The IF5 front panel has four ports. To access three of the ports, you need to remove the cable access door.

To remove the access door

- On the underside of the IF5, unscrew the two thumbscrews on the cable access door and remove the door.



IF5 Front Panel Ports: *This illustration shows how to remove the cable access door and where the ports are located.*

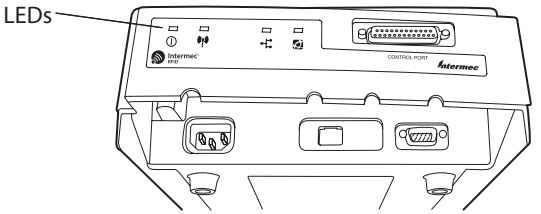
IF5 Front Panel Port Descriptions

Port	Description
AC Power	Used with an appropriate power cable, this port connects the reader to an AC power source.
Ethernet	10BaseT/100BaseTx port. Used with an appropriate cable, this port connects the reader to your Ethernet network. The reader auto-negotiates with the device it is communicating with so that the data rate is set at the highest rate at which both devices can communicate.
Serial	Used with an RS-232 null modem cable (P/N 059167), this port connects the reader to a PC for configuration.
Control	General purpose input/output (GPIO) port. This port connects the reader to industrial controls such as relays or indicators. The port includes optically-isolated inputs, optically-isolated low voltage DC outputs, and access to 12 VDC. For more information on the IF5 GPIO interfaces, see "About the GPIO Interfaces" on page 126.

For more information, see "Port Pin Assignments" on page 137.

Understanding the LEDs

The IF5 has four LEDs that show you the operating status of the reader.



LED Descriptions

LED Icon	LED Name	Description
	Power	Remains on after the IF5 boots.
	Wireless communications	Flashes when a frame is transmitted or received on the 802.11g radio.
	Wired LAN	Flashes when a frame is transmitted or received on the Ethernet port.
	Intermec Ready-To-Work™ Indicator	Blue LED remains on when an application is communicating with the data collection engine (DCE) on the IF5. Blinks when no application is communicating with the DCE. For more information, see the next section.

About the Intermec Ready-To-Work Indicator

The blue Ready-To-Work Indicator shows when an application is communicating with the data collection engine (DCE) on the IF5. The next table explains the different states of the Ready-To-Work indicator.

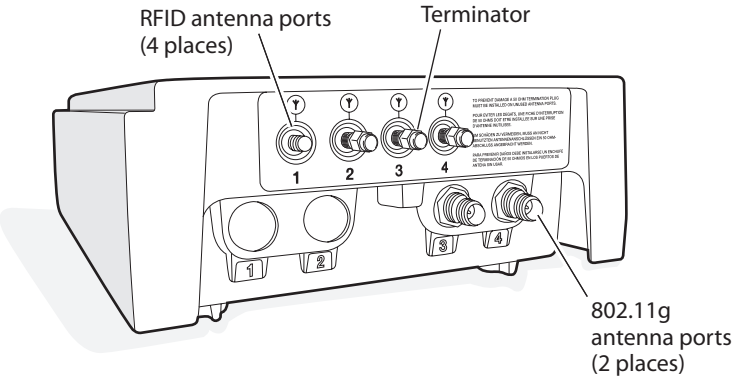
Ready-to-Work Indicator Status Descriptions

Status	Description
Off	IF5 does not have power.
Blinking	No application is communicating with the DCE.
Steady	IF5 developer tools are enabled (default). For more information, see "About IF5 Edgeware" on page 71. Or, the SAP device controller edgeware is enabled. For more information, see "Enabling the SAP Device Controller" on page 140. Or, your custom application is communicating with the DCE. You need to disable the developer tools and the SAP device controller edgeware to use a custom application. For more information, see "About IF5 Edgeware" on page 71.

For more information on the DCE, see "Configuring the Data Collection Engine" on page 80.

Understanding the Rear Panel Ports

The ports on the rear panel are used for connecting the IF5 to RFID and 802.11g radio antennas.



IF5 Rear Panel Ports: *This illustration shows the ports on the rear panel. The IF5 ships with antenna terminators mounted on RFID antenna ports 2, 3, and 4.*

The IF5 RFID antenna ports use these connectors:

- 865-869 MHz: SMA
- 915 MHz: Reverse SMA

Make sure you have appropriate antennas and cables for your IF5. For help, contact your Intermec sales representative.

Caution

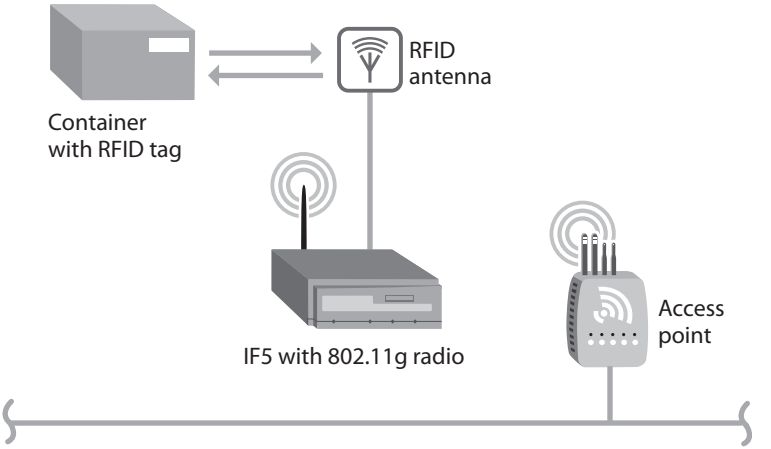
Government regulatory agencies require that this RFID reader only use approved antennas. Therefore, this reader uses a custom antenna connector. Do not use antennas not approved for use with this reader.

Note: The IF5 ships with antenna terminators installed on RFID antenna ports 2, 3, and 4. Do not remove the terminator from any port unless you are installing an antenna or antenna cable on that port.

How the IF5 Fits in Your Network

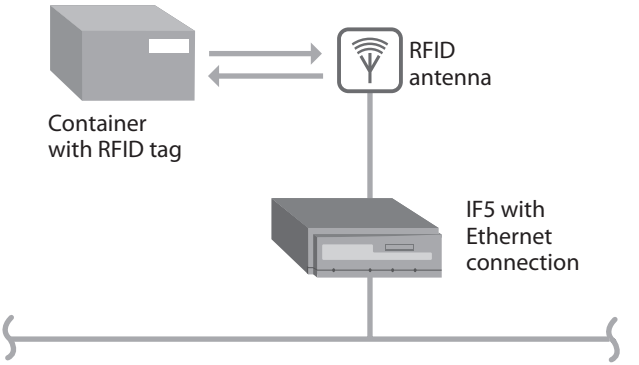
In general, the reader forwards RFID tag data to the wired Ethernet or wireless network. The next illustrations show how the IF5 fits in your network.

IF5 in a Wireless Network



This illustration shows how the IF5 connects to your 802.11g network. The reader communicates with the access point as it sends and receives data from the RFID server.

IF5 in a Wired Ethernet Network



This illustration shows the IF5 in a wired Ethernet network. The IF5 sends and receives RFID tag data to the RFID server through the wired network.

Configuring the IF5 (Setting the IP Address)

By default, the IF5 is configured to be a DHCP client and accepts offers from any DHCP server. Therefore, the IF5 will work out of the box if you are:

- connecting it directly to a wired Ethernet network.
- using a DHCP server to assign it an IP address.

If your IF5 meets these conditions, continue with "Installing the IF5" on page 24.

However, if you are not using a DHCP server to assign an IP address, or if you will be using an 802.11g wireless connection, you need to use a communications program such as HyperTerminal for the initial configuration. For help, see the next section, "Using a Communications Program."

After the IF5 has been assigned an IP address, you can configure, manage, and troubleshoot the IF5 from a remote location using a web browser interface. For help, see "Using the Web Browser Interface" on page 19.

This manual assumes that you are using a communications program for your initial configuration, and then using a web browser interface to perform all other configurations. You can also continue to use a communications program to configure the IF5.

Note: If you need to configure wireless security settings, follow the procedure described in "Using a Communications Program" to assign network parameters to the IF5, and then use the web browser interface to configure security settings.

- For help with using the web browser interface, see "Using the Web Browser Interface" on page 19.
- For help with security, see "Configuring Security" on page 41.

Using a Communications Program

You can use a communications program (such as HyperTerminal) to set the initial IP address for the IF5 and to enable the 802.11g radio. After you configure the IP address, you can continue to use the communications program to set other parameters or you can use a web browser to complete the configuration.

To use a communications program, you must have:

- a terminal or PC with an open serial port and the communications program.
- an RS-232 null-modem cable (P/N 059167). One end of this cable must be a 9-pin socket connector to connect to the serial port on the IF5. To order this cable, contact your local Intermec representative.

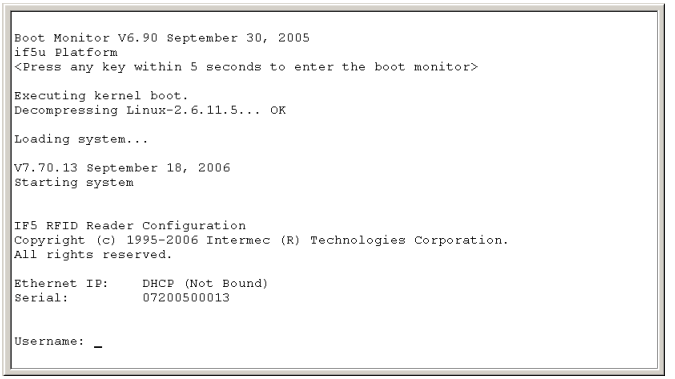
Note: If you have Microsoft ActiveSync running on your desktop PC, you may need to disable ActiveSync to make the serial port available.

To use a communications program

1. Use the RS-232 null-modem cable to connect the serial port on the IF5 to a serial port on your PC.
2. Start the communications program and configure the serial port communications parameters on your PC, and then click **OK**. You should configure the serial port communications parameters to:

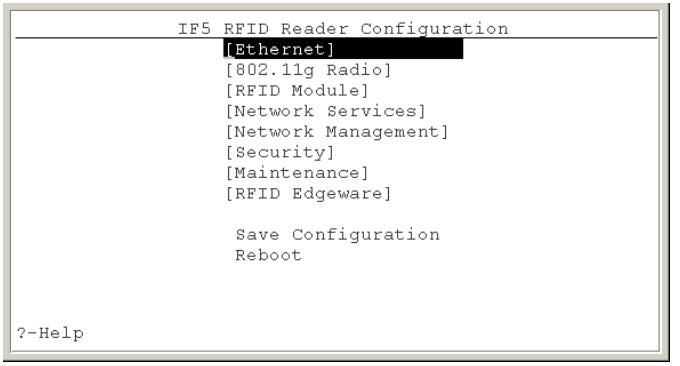
Bits per second	9600
Data bits	8
Parity	None
Stop bit	1
Flow control	None

3. Connect the IF5 to AC power. The IF5 boots as soon as you apply power.
4. Press **Enter** when the message "Starting system" appears on your screen. The **Username** field appears.



5 In the **Username** field type the default user name `intermec`, and then press **Enter**.

6 In the **Password** field type the default password `intermec`, and then press **Enter**. The IF5 RFID Reader Configuration menu appears.



To configure the IF5 for a wired Ethernet connection, continue with the next procedure.

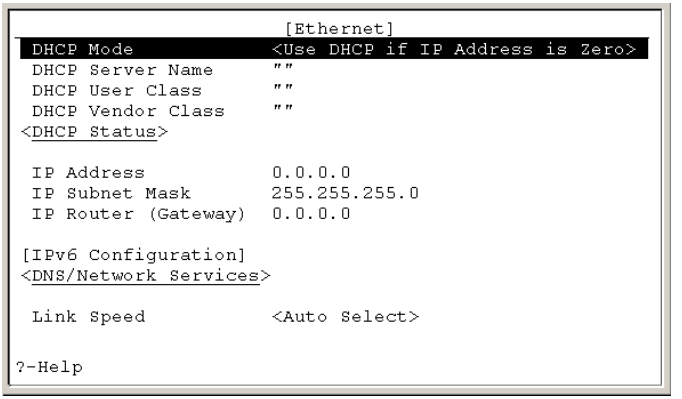
To configure the IF5 for an 802.11g radio connection, continue with "Configuring the IF5 for a Wireless Network" on page 15.

Configuring the IF5 for an Ethernet Connection

Follow this procedure to configure the IF5 for a wired Ethernet connection that does not use a DHCP server. If your wired network uses a DHCP server, continue with "Connecting the IF5 to Your Network" on page 25.

To configure the IF5 for a wired Ethernet connection

1. Connect to the IF5 using a communications program. For help, see "To use a communications program" on page 11.
2. With **Ethernet** selected in the IF5 RFID Reader Configuration menu, press the right arrow key. The Ethernet menu appears.



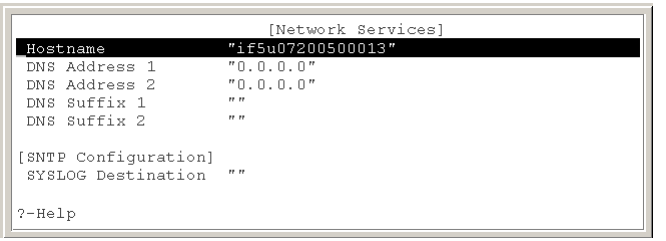
3. Configure these settings:

DHCP Mode	Set to **Disable DHCP**.
IP Address	A unique IP address.
IP Subnet Mask	The subnet mask that matches the other devices in your network.
IP Router (Gateway)	If the IF5 will communicate with devices on another subnet, enter the address of the router that will forward frames.

Or, press the down arrow key to select **IPv6 Configuration**, and then press the right arrow key to configure these IPv6 settings:

Enable Autoconfiguration	Enables automatic assignment of a unique address to this IF5.
IPv6 Address	A unique 128-bit IPv6 address.
IPv6 Subnet Mask	The IPv6 subnet mask. Range is 1 to 128 bits.
IPv6 Router (Gateway)	A unique 128-bit address for an IPv6 router.

4 (Optional) To configure DNS settings, choose **DNS/ Network Services** and press **Enter**. The Network Settings screen appears.



Configure DNS settings as needed:

Hostname	Hostname for this IF5. The default is the IF5 configuration string found on the product label. This can be a simple hostname or a fully qualified domain name (FQDN). If this device obtains its IP address via DHCP, this parameter is also sent to the DHCP server. If the DHCP server supports it, this field will be used for dynamic DNS (DDNS) updates.
Domain name	Specifies a domain name representing this IF5. If the IF5 obtains its IP address via DHCP, this parameter is combined with the hostname parameter and sent to the DHCP server. If the DHCP server supports it, this value is used for dynamic DNS (DDNS) updates.
DNS Address 1	IP address of a domain name server that the IF5 uses to resolve DNS names.

DNS Address 2	IP address of a domain name server that the IF5 uses to resolve DNS names if the DNS server at DNS Address 1 is not responding.
DNS Suffix 1	Domain name suffix that will be appended to DNS names that cannot be resolved.
DNS Suffix 2	Domain name suffix that will be appended to DNS names that cannot be resolved either by themselves or using DNS suffix 1.

5. Press the left arrow key to return to the main reader configuration menu.
6. Press the down arrow key to select **Save Configuration** and then press **Enter**. The new settings are saved.
7. Press the down arrow key to select **Reboot** and then press **Enter**. The IF5 reboots. When the boot process is finished, you see "Starting system" at the bottom of the HyperTerminal screen.
8. Disconnect the null-modem cable and AC power cable from the IF5.

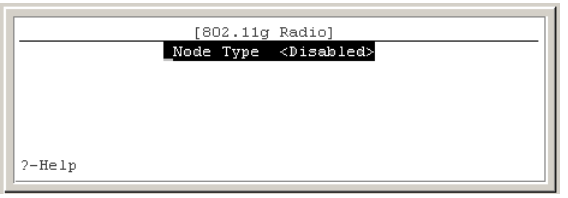
The IF5 is now ready to be connected to your network. See "Connecting the IF5 to Your Network" on page 25.

Configuring the IF5 for a Wireless Network

Follow this procedure to configure the IF5 for connection to a wireless network.

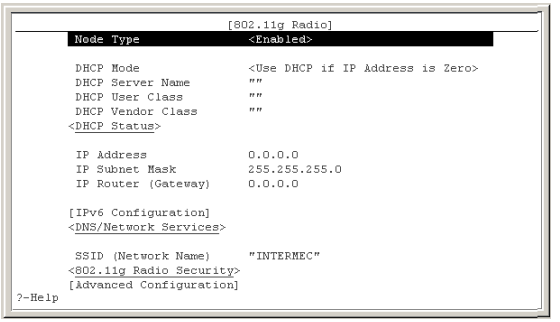
To configure the IF5 for an 802.11g connection

1. Connect to the IF5 using a communications program. For help, see "To use a communications program" on page 11.
2. In the IF5 RFID Reader Configuration menu, press the down arrow key to choose **802.11g Radio** and then press **Enter**. The 802.11g Radio screen appears, with **Node Type** set to **Disabled**.



3 Press the right arrow key. The Node Type list appears.

4 Press the up arrow key to choose **Enabled** from the list and then press **Enter**. The 802.11g Radio screen appears with the complete list of radio settings.



If you are using a DHCP server, configure these settings:

DHCP Server Name	Name of the DHCP server. The IF5 will accept DHCP lease offers from this server only.
DHCP User Class	(Optional) User class for this DHCP server.
DHCP Vendor Class	(Optional) Vendor class for this DHCP server.
SSID (Network Name)	Name of your wireless network. The IF5 will connect to this network only.

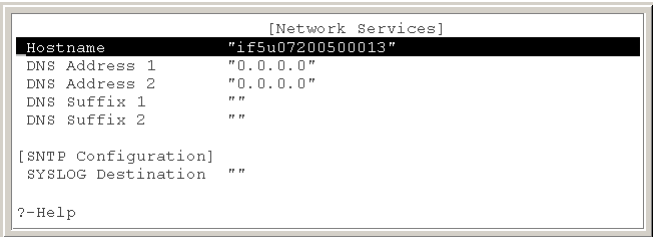
If you are not using a DHCP server, you need to assign network parameters. Configure these settings:

DHCP Mode	Set to **Disable DHCP**.
IP Address	A unique IP address for this IF5.
IP Subnet Mask	The subnet mask that matches the other devices in your network.
IP Router (Gateway)	If the IF5 will communicate with devices on another subnet, enter the address of the router that will forward frames.
SSID (Network Name)	Name of your wireless network. The IF5 will connect to this network only.

Or, press the down arrow key to select **IPv6 Configuration**, and then press the right arrow key to configure IPv6 settings:

Enable Autoconfiguration	Enables automatic assignment of a unique address to this IF5.
IPv6 Address	A unique 128-bit IPv6 address.
IPv6 Subnet Mask	The IPv6 subnet mask. Range is 1 to 128 bits.
IPv6 Router (Gateway)	A unique 128-bit address for an IPv6 router.

5 (Optional) To configure DNS settings, choose **DNS/ Network Services** and press **Enter**. The Network Settings screen appears.



Configure DNS settings as needed:

Hostname Hostname for this IF5. The default is the IF5 configuration string found on the product label.

This can be a simple hostname or a fully qualified domain name (FQDN). If this device obtains its IP address via DHCP, this parameter is also sent to the DHCP server. If the DHCP server supports it, this field will be used for dynamic DNS (DDNS) updates.

Domain name Specifies a domain name representing this IF5. If the IF5 obtains its IP address via DHCP, this parameter is combined with the hostname parameter and sent to the DHCP server. If the DHCP server supports it, this value is used for dynamic DNS (DDNS) updates.

DNS Address 1 IP address of a domain name server that the IF5 uses to resolve DNS names.

DNS Address 2 IP address of a domain name server that the IF5 uses to resolve DNS names if the DNS server at DNS Address 1 is not responding.

DNS Suffix 1 Domain name suffix that will be appended to DNS names that cannot be resolved.

DNS Suffix 2 Domain name suffix that will be appended to DNS names that cannot be resolved either by themselves or using DNS suffix 1.

6 Press the left arrow key to return to the main reader configuration menu.

7 Press the down arrow key to select **Save Configuration** and then press **Enter**. The new settings are saved.

8 Press the down arrow key to select **Reboot** and then press **Enter**. The IF5 reboots. When the boot process is finished, you see "Starting system" at the bottom of the HyperTerminal screen.

9 Disconnect the null-modem cable and AC power cable from the IF5.

The IF5 is now ready to be connected to your wireless network. See "Connecting the IF5 to Your Network" on page 25.

Using the Web Browser Interface

After you have set the initial IP address, you can configure and manage the IF5 remotely using the web browser interface. The IF5 web browser interface has been tested using Internet Explorer 6.0. Using other browsers may provide unpredictable results.

To use the web browser interface, the IF5 must be connected to your wired Ethernet or 802.11g wireless network.

If your session terminates abruptly or a new login screen appears, someone else may have accessed the IF5. When using the web browser interface, remember that your session terminates if you do not use it for 15 minutes.

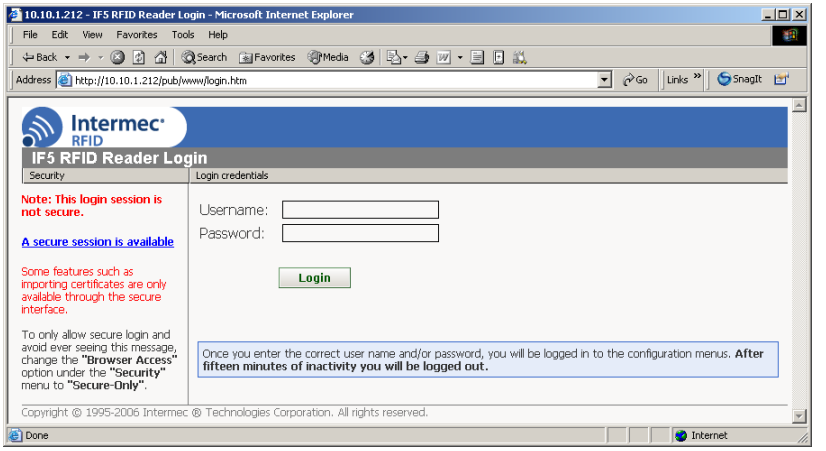
Note: If you access the Internet using a proxy server, add the IF5 IP address to your Exceptions list. The Exceptions list contains the addresses that you do not want to use with a proxy server.

To use the IF5 web browser interface

1 Determine the IP address of the IF5. If a DHCP server assigned the IP address, you need to get the IP address from that server.

2 Start Internet Explorer.

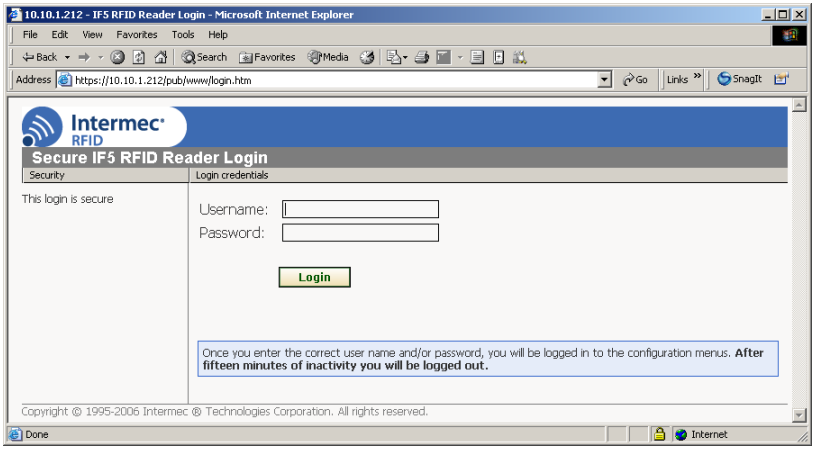
3 In the **Address** field, enter the IP address, and press **Enter**. The IF5 login screen appears.


10.10.1.212 - IF5 RFID Reader Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.1.212/pub/www/login.htm
Intermec RFID
IF5 RFID Reader Login
Security
Login credentials
Note: This login session is not secure.
A secure session is available
Some features such as importing certificates are only available through the secure interface.
To only allow secure login and avoid ever seeing this message, change the "Browser Access" option under the "Security" menu to "Secure-Only".
Username:
Password:
Login
Once you enter the correct user name and/or password, you will be logged in to the configuration menus. After fifteen minutes of inactivity you will be logged out.
Copyright © 1995-2006 Intermec ® Technologies Corporation. All rights reserved.
Done
Internet

Or, for a secure session, click **A secure session is available**. The secure login screen appears.

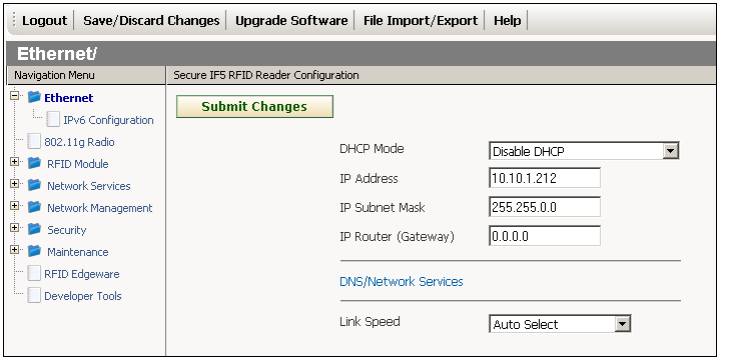
Note: If a security alert message appears:

- Click **Yes** to continue to the secure login screen.
- Click **No** to cancel.
- Click **View certificate** to see the security certificate before continuing.


10.10.1.212 - IF5 RFID Reader Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://10.10.1.212/pub/www/login.htm
Intermec RFID
Secure IF5 RFID Reader Login
Security
Login credentials
This login is secure
Username:
Password:
Login
Once you enter the correct user name and/or password, you will be logged in to the configuration menus. After fifteen minutes of inactivity you will be logged out.
Copyright © 1995-2006 Intermec ® Technologies Corporation. All rights reserved.
Done
Internet

4 If necessary, enter a user name and password. The default user name is `intermec` and the default password is `intermec`. You can define the user name and password. For help, see "Setting Up Logins" on page 45.

5 Click **Login**. The Ethernet screen appears.



Ethernet Screen: *Different settings appear in this screen depending on DHCP settings. These settings appear when the IF5 is configured to use a DHCP server.*

Your web browser session is established.

Note: Although you can use several methods to manage the IF5 remotely, this manual assumes you are using the web browser.

Saving Configuration Changes

When you are done configuring the IF5, you may want to activate your changes immediately or you may want to save the changes now and activate them later. If you choose to activate the changes later, they will become active the next time the IF5 is booted.

Note: If you made changes to RFID module settings, you need to reboot the IF5 to activate those changes.

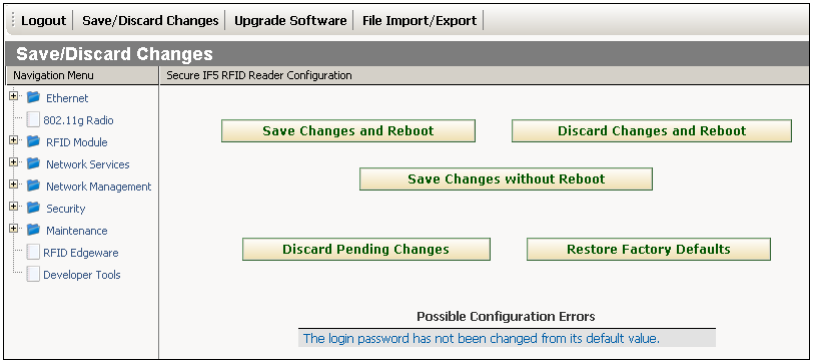
IF5 Configuration Files

Configuration File	Description
Default	This configuration file is the factory default configuration. For help, see "Restoring the IF5 to the Default Configuration" on page 118.
Current	When you click **Submit Changes**, the IF5 updates the current configuration file. The IF5 does not change the active configuration file. You can see a list of pending changes when you click **Save/Discard Changes**. Having separate files for the current and active configurations lets you make changes while the IF5 is running without interrupting communication.
Active	When you click **Save/Discard Changes** > **Save Changes and Reboot**, the IF5 copies the current configuration file to the active configuration file. The active configuration file is the file that the IF5 uses.

To save or discard configuration changes

1 On the menu bar, click **Save/Discard Changes**.

The Save/Discard Changes screen appears.



2 To discard changes, click **Discard Pending Changes**.

To save changes, continue with the next step.

3 Verify that all your configuration changes appear in the Pending Changes list.

4 Click **Save Changes and Reboot** to reboot the IF5 and immediately use your new active configuration.

Or, click **Save Changes without Reboot**. The IF5 saves the changes to its current configuration and continues to run its active configuration. You will need to reboot the IF5 when you want the current configuration to become the active configuration.

Installing the IF5

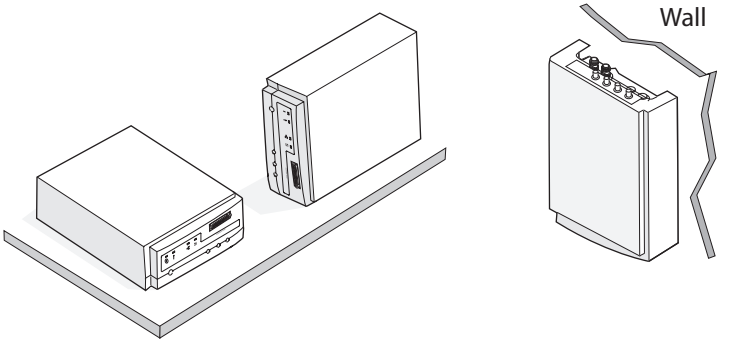
This section explains how to choose a mounting location for the IF5 and connect the IF5 to your wired Ethernet or wireless network.

Choosing a Mounting Location

You can place the IF5 horizontally or vertically on a stable surface. You can also mount the IF5 to a wall or a beam using one of these mounting bracket kits:

- Mounting bracket kit (P/N 068918)
- Rotating mounting bracket kit (P/N 068751)

For more information, contact your local Intermec representative.



Mounting the IF5: *This illustration shows the ways you can install the IF5 on a horizontal or vertical surface.*

The next table includes environmental requirements for the IF5. Choose a location that meets these requirements.

IF5 Environmental Requirements

Type	Minimum	Maximum
Operating temperature	-25ºC (-13ºF)	55ºC (131ºF)
Storage temperature	-30ºC (-22ºF)	75ºC (167ºF)
Humidity (non-condensing)	10%	90%

Connecting the IF5 to Your Network

After you configure the IF5 for your network and choose a mounting location, you can place the IF5 in its mounting location and connect it to your network.

For help with configuring the IF5, see "Configuring the IF5 (Setting the IP Address)" on page 10.

Note: If you are using a DHCP server, make sure the server is running before you connect power to the IF5. If there is no DHCP server available at boot time, the IF5 may seem to be locked up while searching for DHCP lease offers.

To install the IF5

1. Remove the cable access door. For help, see "Understanding the Front Panel Ports" on page 4.
2. Attach one to four RFID antennas to the RFID antenna ports, starting with port 1. Do not remove the terminators from unused antenna ports. For help, see "Understanding the Rear Panel Ports" on page 8.

Each port must have either an antenna or a terminator connected. Do not apply power to the reader unless an antenna or terminator is installed on each antenna port.

3. For a wired Ethernet network, connect an Ethernet cable to the IF5 Ethernet port.

   For a wireless network, install the primary 802.11g radio antenna on antenna port 4. You can connect a secondary 802.11g antenna to port 3.
4. Connect the AC power cord to the power port on the IF5.

Note: The IF5 does not support power over Ethernet (POE).

5. Install the cable access door and route the cables through the openings in the door seam. Make sure the cables are not caught in the seam.

6 Place the IF5 in its mounting location. For more information, see "Choosing a Mounting Location" on page 24.

7 For a wired Ethernet network, connect the Ethernet cable to your network.

   For a wireless network, continue with the next step.

8 Connect the AC power cord to an AC outlet. As soon as you apply power, the IF5 boots and the green Power LED turns on.

The IF5 is now ready to communicate in your network.

Positioning 802.11g Antennas

Antennas and their placement play a vital role when installing a wireless network. The exact range that you will achieve is difficult to determine. Intermec recommends that you allow an Intermec-certified RF specialist to perform a site survey before you install a wireless network. For more information, contact your local Intermec representative.

Radio signals may reflect off some obstacles and be absorbed by others. For example, two radios may achieve up to 305 m (1,000 ft) of range if positioned outdoors within line of sight, with no obstacles between them. However, the same two radios may only achieve 152 m (500 ft) of range when the RF signal has to travel through items such as cubicles. If the signal must penetrate office walls, the signal range may decrease to 91 m (300 ft).

Using the proper antennas for your environment and placing them in the proper areas can help improve range. Here are some general guidelines for positioning antennas:

- Place the antenna as high as possible. In an office environment, try to place it above cubicle walls.
- Keep the line-of-sight between the antennas and wireless end devices clear of metal surfaces (like beams or girders) and large quantities of paper products.
- Do not place items constructed from sheet metal (such as filing cabinets) between two antennas.

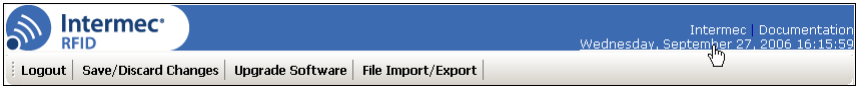
Setting the Date and Time

After you have installed the IF5, you can set the date and time via the web browser interface.

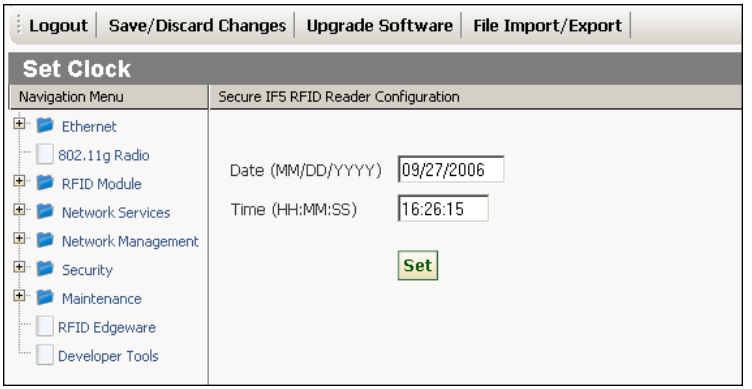
To set the date and time

1 Connect to the IF5 via the web browser interface. For help, see "Using the Web Browser Interface" on page 19.

2 In the web browser screen, click the date and time in the upper right-hand corner.


Intermec RFID
Intermec | Documentation
Wednesday, September 27, 2006 16:15:59
Logout | Save/Discard Changes | Upgrade Software | File Import/Export

The Set Clock screen appears.



3 In the **Date** field, enter the current date using the format *mm/dd/yyyy*, where:

mm is the month.

dd is the date.

yyyy is the year.

4 In the **Time** field, enter the current time using the format *hh:mm:ss*, where:

hh is the correct hour in UTC (24-hour) format.

mm is the correct minute.

ss is the correct second.

5 Click **Set**. The IF5 date and time are set.

Using the IF5 Securely

To help protect the integrity and security of your data, the IF5 supports a variety of secure access methods. You can:

- use a secure web browser session (HTTPS) to access the IF5. For help, see "Using the Web Browser Interface" on page 19.
- limit developer access to the IF5 by disabling the IF5 FTP server or its NFS shared drive. For help, see "Controlling Developer Access" on page 44.
- disable Telnet access to the IF5. For help, see "Controlling Developer Access" on page 44.
- configure and use network security methods. For help, see "Configuring Security" on page 41.

2 Configuring Network Settings

This chapter describes how to configure network settings for the IF5 and includes these topics:

- Configuring Settings For Your Network
- Configuring Ethernet Settings
- Configuring Network Services
- Configuring the 802.11g Radio
- Configuring Security
- About Certificates

This chapter assumes that you are familiar with your network, networking terms, and the type of security implemented by your network.

Configuring Settings for Your Network

This chapter assumes that you are using the IF5 web browser interface to configure network settings on the IF5. For help, see "Using the Web Browser Interface" on page 19.

You can also configure network settings by:

- using a communications program to access the IF5. For help, see "Using a Communications Program" on page 10.
- using Intermec Settings from within the Intermec SmartSystems™ Console. For help, see "Using the Intermec SmartSystems Console" on page 103.
- using a Simple Management Network Protocol (SNMP) station to access the IF5. For help, see "Using Simple Network Management Protocol (SNMP)" on page 98.
- using the Wavelink Avalanche client management system to access the IF5. For help, see "Using Wavelink Avalanche" on page 101.

Configuring Ethernet Settings

This section explains how to configure these wired Ethernet settings using the web browser interface:

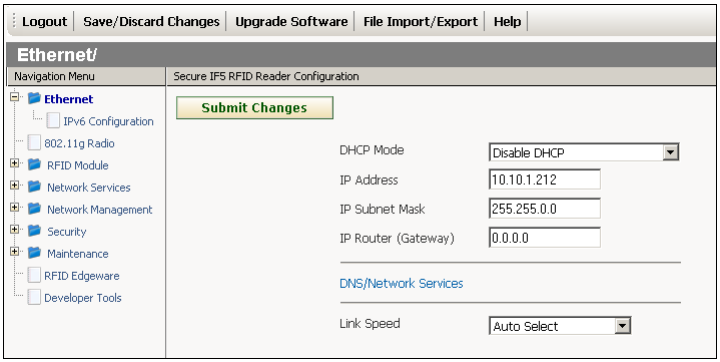
- DHCP mode
- (If DHCP is enabled) DHCP server name, user class, and vendor class
- IP address
- IP subnet mask
- IP router (gateway)
- Link speed

Note: If you are using a DHCP server, you may not need to configure Ethernet settings. For more information, contact your network administrator.

For help with enabling IPv6 and configuring settings, see "Enabling IPv6" on page 33.

To configure Ethernet settings

1 From the menu, click **Ethernet**. The Ethernet screen appears.



2 Configure the Ethernet settings. For help, see the next table.

Note: Different settings appear in this screen depending on the current DHCP mode for the IF5.

If you need to configure DNS/Network Services settings such as DNS addresses or suffixes, or a SYSLOG destination, see "Configuring Network Services" on page 34.

3 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

Ethernet Setting Descriptions

Parameter	Description
DHCP Mode	Sets the DHCP mode for this IF5: • Choose **Always Use DHCP** if you want the IF5 to get its IP address from a DHCP server. • Choose **Use DHCP if IP Address is Zero** if you want the IF5 to use DHCP whenever its IP address is set to 0.0.0.0. If you choose this option, make sure the IP Address is set to 0.0.0.0 • Choose **Disable DHCP** if you want to assign a static IP address to the IF5.
DHCP Server Name	Name of the DHCP server. The IF5 accepts lease offers from only this server.
DHCP User Class	(Optional) User class for this DHCP server.
DHCP Vendor Class	(Optional) Vendor class for this DHCP server.
IP Address	IP address of the IF5 Ethernet connection. The IP address has the form *x.x.x.x*, where *x* is a number from 0 to 255. Set this value to 0.0.0.0 if you set the DHCP Mode to **Use DHCP if IP Address is Zero**. Set this value to a static IP address for the Ethernet connection if you disabled DHCP.
IP Subnet Mask	Subnet mask for this network. The subnet mask has the form *x.x.x.x*, where *x* is a number from 0 to 255.
IP Router (Gateway)	IP address of the router. The IP address has the form *x.x.x.x*, where *x* is a number from 0 to 255.
Link Speed	Choose the speed and duplex mode you want the IF5 to use when it communicates with the Ethernet network. If you want the IF5 to auto-negotiate this field, choose **Auto Select**. Auto Select should work for most networks.

Enabling IPv6

1. To enable IPv6 for your Ethernet connection, in the menu click **Ethernet** > **IPv6 Configuration**. Or, to enable IPv6 for the 802.11g radio connection, click **802.11g Radio** > **IPv6 Configuration**. The IPv6 Configuration screen appears.
2. Check the check box to enable IPv6, or uncheck the check box to disable IPv6.
3. Click **Submit Changes** to save your changes. The IPv6 Configuration screen appears.
4. If you want to enable IPv6 autoconfiguration, click **Enable Autoconfiguration** and continue with Step 5.

   If you do not want to enable IPv6 autoconfiguration:

   a. Click **Submit Changes**. The screen refreshes with a list of IPv6 configuration settings.

   b. Configure IPv6 settings. For help, see the next table.
5. Click **Submit Changes**. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

IPv6 Setting Descriptions

Parameter	Description
IPv6 Address	A unique 128-bit IPv6 address.
IPv6 Subnet Mask	The IPv6 subnet mask. Range is 1 to 128 bits.
IPv6 Router (Gateway)	A unique 128-bit address for an IPv6 router.

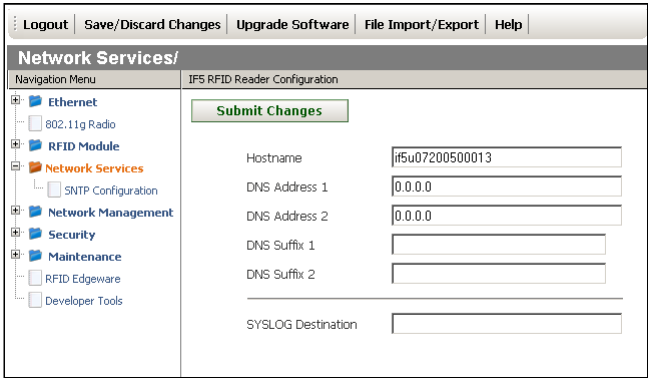
Configuring Network Services

This section explains how to configure these network service settings using the web browser interface:

- Hostname
- Domain name
- Domain Name Server (DNS) addresses 1 and 2
- DNS suffixes 1 and 2
- SYSLOG destination

To configure network services

1. In the menu, click **Network Services**. Or, in the 802.11g Radio screen or the Ethernet screen, click **DNS/Network Services**. The Network Services screen appears.



2. Configure settings. For help, see the next table.
3. Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

Network Services Setting Descriptions

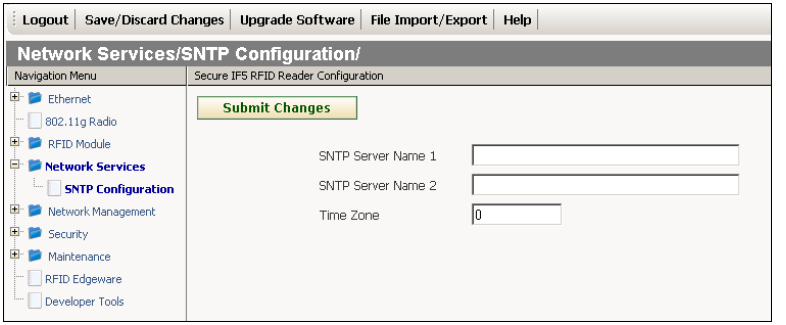
Parameter	Description
Hostname	Name for this device. The default is the configuration string for this IF5. The hostname can be either a simple hostname, or a qualified domain name (FQDN). If this device obtains its IP address via DHCP, this parameter is sent to the DHCP server. If the server supports it, this field is used for dynamic DNS updates.
Domain name	Specifies a domain name representing this IF5. If the IF5 obtains its IP address via DHCP, this parameter is combined with the hostname parameter and sent to the DHCP server. If the DHCP server supports it, this value is used for dynamic DNS (DDNS) updates.
DNS Address 1	Enter the IP address of a domain name server that the IF5 uses to resolve DNS names.
DNS Address 2	Enter the IP address of a domain name server that the IF5 uses to resolve DNS names if the DNS server at DNS Address 1 is not responding.
DNS Suffix 1	Enter a domain name suffix that will be appended to DNS names that cannot be resolved.
DNS Suffix 2	Enter a domain name suffix that will be appended to DNS names that cannot be resolved either by themselves or using DNS suffix 1.
SYSLOG Destination	Domain name or IP address of the SYSLOG server. In Unix networks, system messages are logged to this server.

Configuring SNTP Client Settings

This section explains how to configure Simple Network Time Protocol (SNTP) client parameters. For information on public NTP servers, see http://ntp.isc.org.

To configure SNTP settings

1 In the menu, click **Network Services > SNTP Configuration**. The SNTP Configuration screen appears.



2 Enter SNTP information:

- In the **SNTP Server Name 1** and **SNTP Server Name 2** fields, enter the DNS name or IP address of an SNTP or NTP server.
- In the **Time Zone** field, enter a signed integer that represents the offset of your time zone, in hours, from Coordinated Universal Time (UTC). A positive integer represents a location east of the zero meridian and a negative integer indicates a location west of the zero meridian.

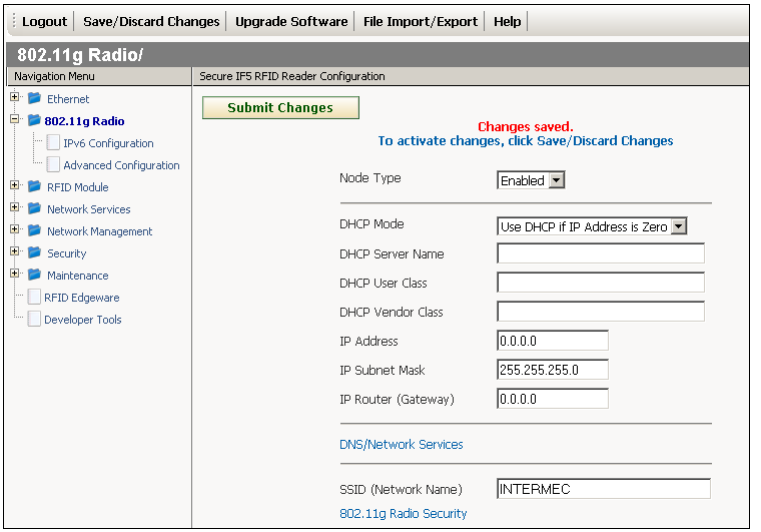
3 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

Configuring the 802.11g Radio

This section explains how to configure settings for the 802.11g radio.

To configure the radio

1 In the main menu, click **802.11g Radio**. The 802.11g Radio screen appears:



Note: If the radio is disabled, choose **Enable** from the **Node Type** drop-down list, and then click **Submit Changes** to see the complete 802.11g Radio screen.

2 Configure the parameters for the radio. For help, see the next table.

3 (Optional) If you need to configure network services settings such as DNS addresses or suffixes, or a SYSLOG destination, see "Configuring Network Services" on page 34.

4 (Optional) If you need to configure Internet Protocol version 6, see "Enabling IPv6" on page 33.

5 (Optional) If you need to configure security, see "Configuring Security" on page 41.

6 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

802.11g Radio Settings Descriptions

Setting	Description
Node Type	Enables or disables the radio.
DHCP Mode	Sets the DHCP mode for this IF5: • Choose **Always Use DHCP** if you want the IF5 to get its IP address from a DHCP server. • Choose **Use DHCP if IP Address is Zero** if you want the IF5 to use DHCP whenever its IP address is set to 0.0.0.0. If you choose this option, make sure the IP Address is set to 0.0.0.0 • Choose **Disable DHCP** if you want to assign a static IP address to the IF5. If you choose this option, be sure you set a static IP address in the IP Address field.
DHCP Server Name	Name of the DHCP server (up to 31 characters). The IF5 responds only to DHCP offers from this server. Default is an empty string (the IF5 responds to DHCP offers from any server).
DHCP User Class	DHCP user class identifier. A DHCP server uses the User Class option to choose the address pool it allocates an address from and to select other configuration options. Default is an empty string (the IF5 does not include user class information in DHCP requests).

802.11g Radio Settings Descriptions (continued)

Setting	Description
DHCP Vendor Class	DHCP vendor class identifier. A DHCP server can assign vendor-specific options to DHCP clients that have a common vendor. Default is an empty string (the IF5 does not include vendor class information in DHCP requests).
IP Address	IP address for the 802.11g radio. The IP address has the form *x.x.x.x*, where *x* is a number from 0 to 255. Set this value to 0.0.0.0 if you set the DHCP Mode to **Use DHCP if IP Address is Zero**. Set this value to a static IP address for the 802.11g radio if you disabled DHCP.
IP Subnet Mask	Subnet mask that matches the other devices in your network. The subnet mask has the form *x.x.x.x*, where *x* is a number from 0 to 255.
IP Router (Gateway)	IP address of the router that will forward frames if the IF5 will communicate with devices on another subnet. The IP address has the form *x.x.x.x*, where *x* is a number from 0 to 255.
SSID (Network Name)	Name of the network. The IF5 will only connect to the specified network.

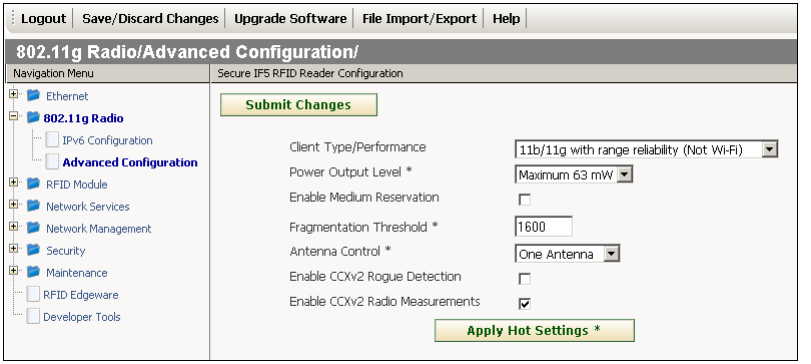
Configuring Advanced Parameters

You can change these settings to enable better radio performance.

Note: Intermec recommends that you keep the default settings for these parameters.

To configure advanced radio parameters

1 From the menu, click **802.11g Radio > Advanced Configuration**. The Advanced Configuration screen appears.



Parameters marked with an asterisk (*) are considered "hot settings," meaning that their values can be changed and immediately applied without rebooting the IF5.

2 Configure the advanced parameters. For help, see the next table.

3 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

Or, click **Apply Hot Settings** to immediately apply the Power Output Level, Fragmentation Threshold, and Antenna Control settings.

802.11g Radio Advanced Parameters

Parameter	Description
Client Type/ Performance	Determines the client type and data rate set for the 802.11g radio.
Power Output Level	Sets the transmitter power output level.
Enable Medium Reservation	Determines if you want to specify a reservation threshold. Check this check box to set a threshold value.
Fragmentation Threshold	Size of the largest data packet that can be transmitted without fragmentation. Default is 1600 bytes.

802.11g Radio Advanced Parameters

Parameter	Description
Antenna Control	Choose **One Antenna** to use only the antenna connected to Antenna Port 4 for both transmission and reception. Choose **Two Antennas** to allow the radio to select the transmitting antenna, based on best reception. You should connect a second antenna to Antenna Port 3 if you want to choose this option.
Enable CCXv2 Rogue Detection	If you are using Cisco access points, check this check box to allow CCXv2 rogue access point detection.
Enable CCxv2 Radio Measurements	If you are using Cisco access points, check this check box to allow CCxv2 radio measurement responses.

Configuring Security

Note: Before you configure security settings for this IF5, you should be familiar with the type of security implemented for your network.

The IF5 supports a variety of security features to help maintain the integrity of your secure network. You can:

- change default network parameters. For help, see "Configuring the 802.11g Radio" on page 37.
- enable/disable access methods. For example, if you are not using Telnet sessions to configure or manage the IF5, you can disable Telnet access. For help, see the next section, "Controlling Access to IF5 Menus," or see "Controlling Developer Access" on page 44.
- change the default user name and password. For help, see "Setting Up Logins" on page 45.
- use a password server to maintain a list of authorized users who can configure and manage the IF5. For help, see "Setting Up Logins" on page 45.
- configure basic WEP 64/128 security using static WEP keys. For help, see "Configuring Static WEP Security" on page 50.

- configure Dynamic WEP/802.1x security. For help, see "Configuring Dynamic WEP/802.1x Security" on page 52.
- configure WPA-PSK security. For help, see "Configuring WPA-PSK Security" on page 54.
- configure WPA-802.1x security. For help, see "Configuring WPA-802.1x Security" on page 55.
- configure WPA2-PSK security. For help, see "Configuring WPA2-PSK Security" on page 57.
- configure WPA2-802.1x security. For help, see "Configuring WPA2-802.1x Security" on page 58.

For general information on securely using the IF5, see "Using the IF5 Securely" on page 28.

Controlling Access to IF5 Menus

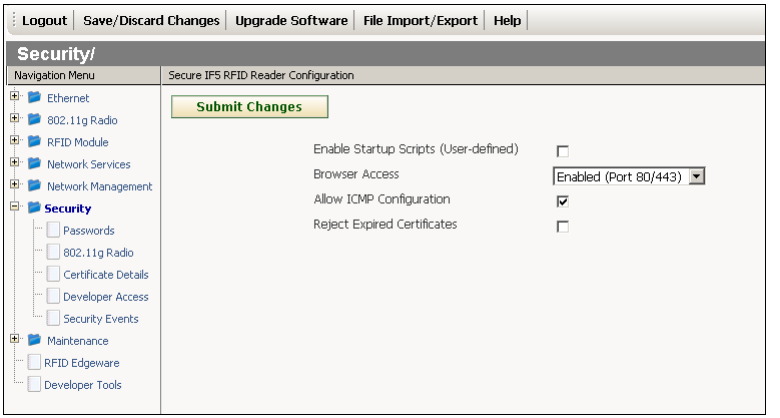
There are two access methods you can enable or disable depending on how you want users to be able to configure or manage the IF5:

- Web browser interface (HTTP or HTTPS)
- Internet Control Message Protocol (ICMP)

Both access methods are enabled by default. You may want to disable any of these methods to prevent unauthorized access.

To enable or disable IF5 access

1 From the menu, click **Security**. The Security screen appears.



2 Enable or disable the access methods that users can use to connect to the IF5. For help, see the next table.

3 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

Access Method Descriptions

Method	Description
Enable Startup Scripts (User-defined)	Enables or disables user-defined startup scripts or applications at boot time. When this box is checked, applications or scripts located in these directories will be run when the IF5 boots: • /home/developer/startup • /cf/startup For more information, see "Running Applications at Boot Time" on page 70.
Browser Access	Determines if users can use a web browser to configure or manage this IF5. Browser access is through either port 80 or port 443. Choose **Secure-Only** if you want users to log in using only the secure web browser (HTTPS) interface. Secure-Only access is through port 443. If you disable browser access to the IF5, you may need to use a communications program to configure and manage the IF5. For help, see "Using a Communications Program" on page 10.
Allow ICMP Configuration	Determines if users can use a program that uses ICMP echo (ping) to set the IP address or restore factory defaults on this IF5.
Reject Expired Certificates	Check this check box if you want the IF5 to reject certificates that have expired. For help, see "About Certificates" on page 61.

Controlling Developer Access

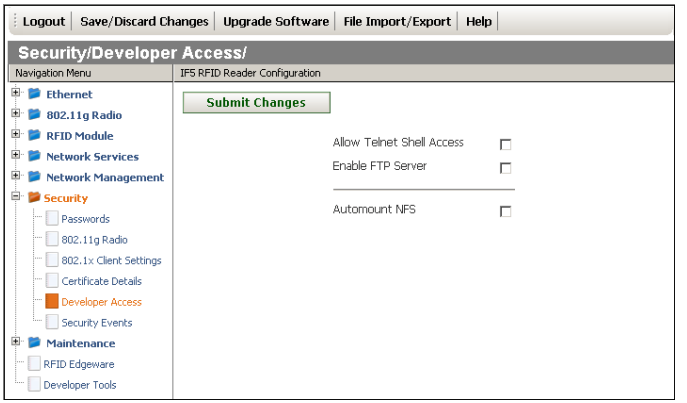
You can control how developers access the IF5 by enabling or disabling these three access methods:

- Via Telnet sessions
- Via FTP server
- Via mounting a Common Internet File System (CIFS)
- Via NFS shared drive

These methods are disabled by default. To enable any of these methods, see the next procedure.

To enable developer access methods

1 From the menu, click **Security** > **Developer Access**. The Security/Developer Access screen appears.



2 Enable or disable developer access methods by checking or clearing the check boxes. For help, see the next table.

3 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

Developer Access Method Descriptions

Method	Description
Allow Telnet Shell Access	Enables access to the Linux system console via standard Telnet, using the login and password `intermec`.
Enable FTP Server	Enables the FTP server, allowing users to transfer files to and from the IF5, using the user name and password `intermec`.
Automount CIFS (SMB)	Enables automatic mounting of a Common Internet File System (CIFS), also known as SMB (server message block) share at boot time. This makes the share accessible via the shell.
Automount NFS	Enables an NFS shared drive when the IF5 is booted. Files on the shared drive are accessible via the shell. If you enable NFS, after you click **Submit Changes**, these fields appear: **Remote Host:** IP address of the NFS server. **Remote Mount Path:** Path to the NFS mount. Specify these settings and click **Submit Changes** again to activate them.

Setting Up Logins

To ensure login security for configuring or maintaining the IF5, you should use a password server or change the default user name and password.

- A password server is typically an embedded authentication server (EAS) or other RADIUS server. To use a password server, you must have a password server on the network that contains the user name/password database. On the IF5, you need to enable RADIUS for login authorization.

  When a user attempts to log in to the IF5, the user must enter a user name and password. This login is sent to the RADIUS server, which compares the login to its list of authorized logins. If a match is found, the user can log in to the IF5 with read/write privileges.

  If no RADIUS server is available when the user tries a login and the **Allow Service Password** check box is checked, the

server checks the service password. If the login does not match the service password, the login fails.

For help, see the next section, "Configuring the IF5 to Use a Password Server."

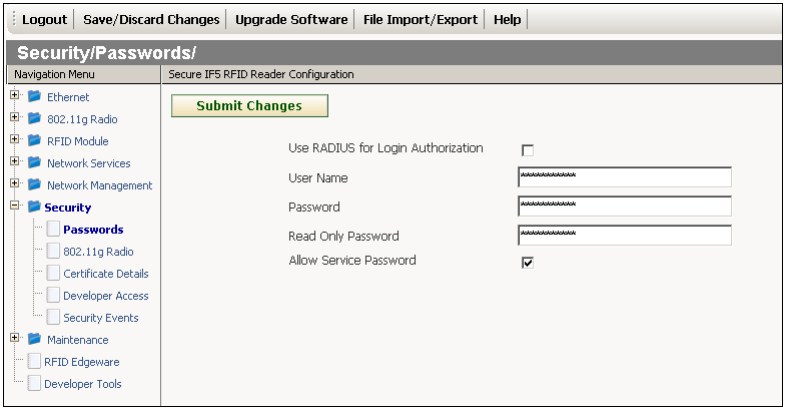
- If you do not want to use a password server, you should change the default login user name and password, and create a read-only password. For help, see "Changing the Default Login" on page 48.

Configuring the IF5 to Use a Password Server

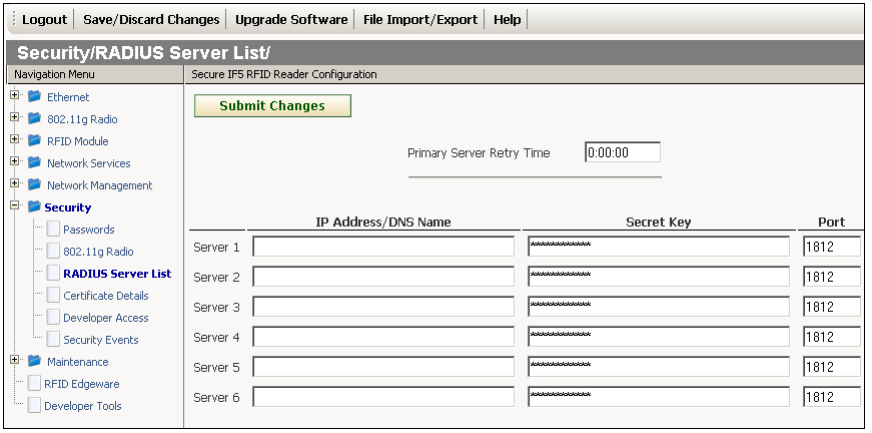
If you use a password server to manage users who can log in to this IF5, you need to tell the IF5 how to communicate with the password server and then you need to configure the password server.

To configure the IF5 to use a password server

1. From the menu, click **Security** > **Passwords**. The Passwords screen appears.



2. Check the **Use RADIUS for login authorization** check box.
3. Click **Submit Changes** to save your changes.
4. Click **Select a RADIUS server for login authorization**. The RADIUS Server List screen appears.



5 Enter RADIUS server information for each password server. For help, see the next table.

Note: If you enter more than one password server, the other password servers act as backup servers. The IF5 uses the first password server (starting with Server 1) whose IP address/DNS name and secret key are the same as one in the list.

6 Configure the password server database. For help, see the documentation that came with your server.

7 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

RADIUS Server Information Descriptions

Type	Description
Primary Server Retry Time	If the RADIUS client is accessing a backup RADIUS server and gets no response, this is the amount of time the client waits before trying to access the primary RADIUS server. A non-zero value causes the RADIUS client to periodically try accessing the primary server to see if it is available. Default is 0.
IP Address/DNS Name	IP address or DNS name of this RADIUS server.

RADIUS Server Information Descriptions (continued)

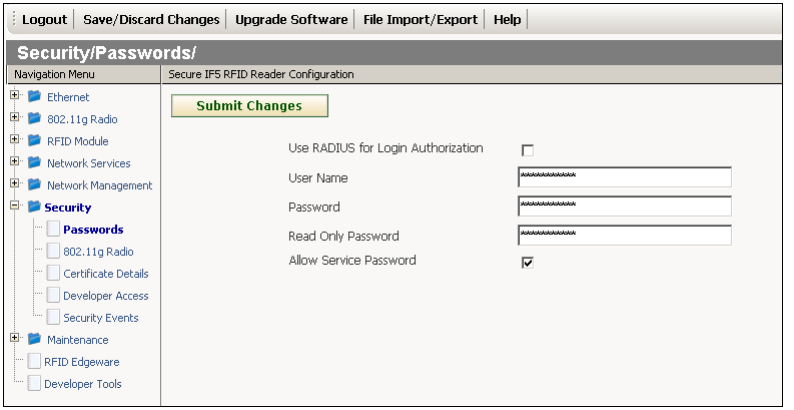
Type	Description
Secret Key	Secret key for this RADIUS server. You can enter the key in ASCII or hex notation. To enter a hexadecimal key, prefix it with "0x".
Port	Port number of this RADIUS server.

Changing the Default Login

If you are not using a password server to authorize user logins, Intermec recommends that you change the default user name and password and create a read-only password.

To set up logins

1 From the main menu, click **Security** > **Passwords**. The Passwords screen appears.



2 Clear the **Use RADIUS for Login Authorization** check box.

3 Click **Submit Changes** to save your changes.

4 Configure the parameters. For help, see the next table.

5 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

Password Parameter Descriptions

Parameter	Description
Use RADIUS for Login Authorization	Determines if you are using a password server to authenticate logins to this IF5. Uncheck this check box if you are not using a password server.
User Name	Enter the user name you need to use to log in to this IF5. The user name can be from 0 to 32 characters long. If you leave the user name and password fields blank, a user will not need to log in to the IF5.
Password	Enter the password you need to use to log in to this IF5. This password gives you read and write access to the IF5 configuration. The password can be from 0 to 32 characters long. If you leave the user name and password fields blank, a user will not need to log in to the IF5.
Read Only Password	Enter the password you need to use to log in to this IF5. This password gives the user read-only access to the IF5. This user can view the configuration and execute diagnostics but cannot perform any tasks that affect IF5 operation, such as changing configuration options or downloading software. To disable this password, delete it.
Allow Service Password	If the user enters a login that does not match either the user name and password or the read only password, this setting (enabled by default) allows the login to be checked against the service password. Intermec Product Support may use this service password if they need to troubleshoot this IF5. If this feature violates your security guidelines, you may disable the service password by unchecking the check box. If you disable the service password and forget your normal password, you will need to contact Product Support for instructions on resetting all passwords to default values.

Configuring Static WEP Security

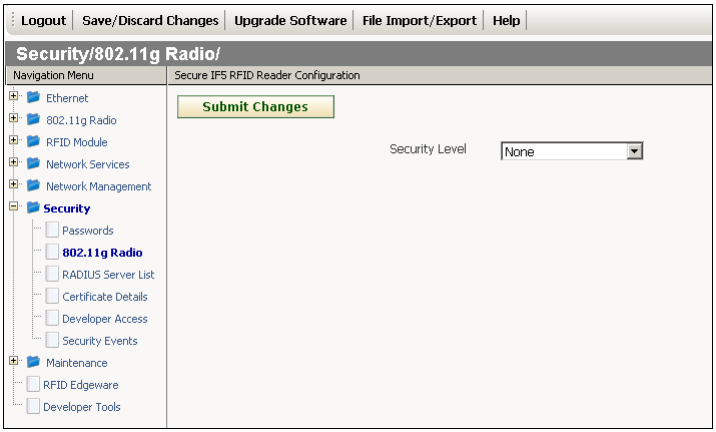
Note: If you configure static WEP security for the IF5, you cannot enable 802.1x authentication for that IF5.

To use static WEP keys, your network must support WEP encryption. All access points and wireless end devices (including this IF5) must use the same WEP encryption type and WEP transmit key. You should periodically change this WEP transmit key to prevent an unauthorized person with a sniffing tool from monitoring your network and discovering the WEP key.

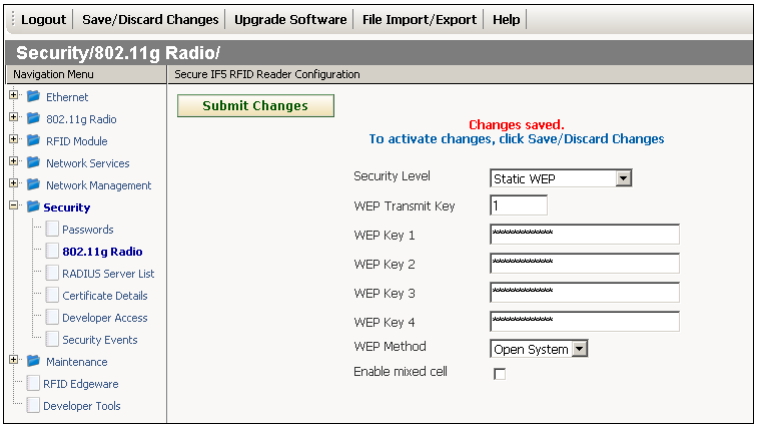
You can enter up to four WEP keys and then pick a WEP transmit key.

To configure WEP security

1 From the menu, click **Security** > **802.11g Radio**. The Security/802.11g Radio screen appears.



2 Choose **Static WEP** from the **Security Level** drop-down list, and then click **Submit Changes**. This screen appears:



3 Configure the parameters for WEP security. To ensure maximum security, configure each WEP key with a different WEP code. For help, see the next table.

4 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

WEP Configuration Parameter Descriptions

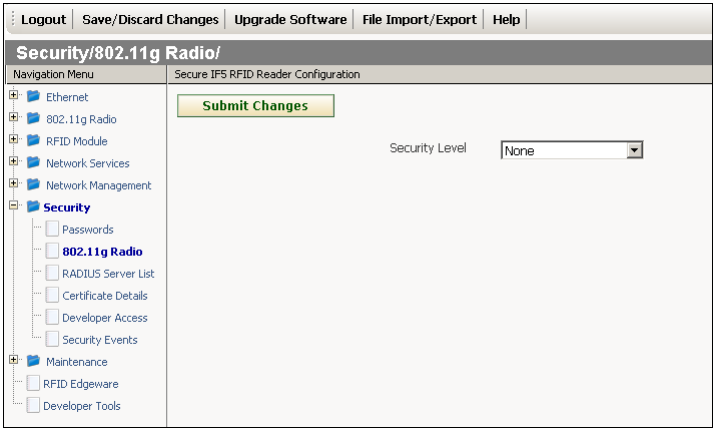
Parameter	Description
WEP Transmit Key	Determines which of the four WEP keys this IF5 uses to transmit data.
WEP Key 1 through WEP Key 4	For WEP 64, enter five ASCII characters or hex pairs. For WEP 128, enter 13 ASCII characters or hex pairs. To enter a key in hex format, precede the hex pairs with 0x. For example, an ASCIIWEP key of ABCDE would be entered in hex format as 0x4142434445.
WEP Method	Specifies whether encryption will be used as part of the authentication algorithm to authenticate the IF5. Choose **Shared Key** to require encryption or **Open System** to require no encryption.
Enable mixed cell	Enable this mode to allow the IF5 to communicate with Cisco access points configured for mixed-cell use. Mixed-cell use allows both WEP and non-WEP clients to communicate with the same access point.

Configuring Dynamic WEP/802.1x Security

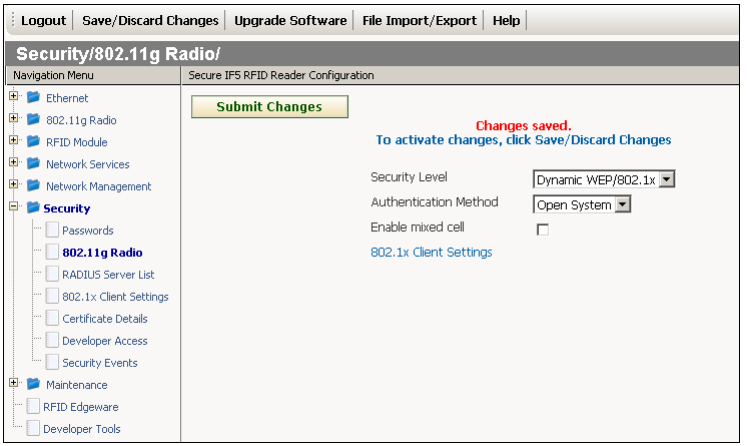
Note: If you enable dynamic WEP security for the IF5, you cannot also enable static WEP keys.

To configure dynamic WEP/802.1x security

1 From the menu, click **Security** > **802.11g Radio**. The Security/802.11g Radio screen appears.



2 Choose **Dynamic WEP/802.1x Security** from the **Security Level** drop-down list, and then click **Submit Changes**. This screen appears:



3 Configure the parameters for Dynamic WEP security. For help, see the next table.

4 Click **802.1x Client Settings**. The Security/802.1x Client Settings screen appears.

5 Configure the 802.1x client settings. For help, see "Configuring 802.1x Client Settings" on page 60.

6 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**,

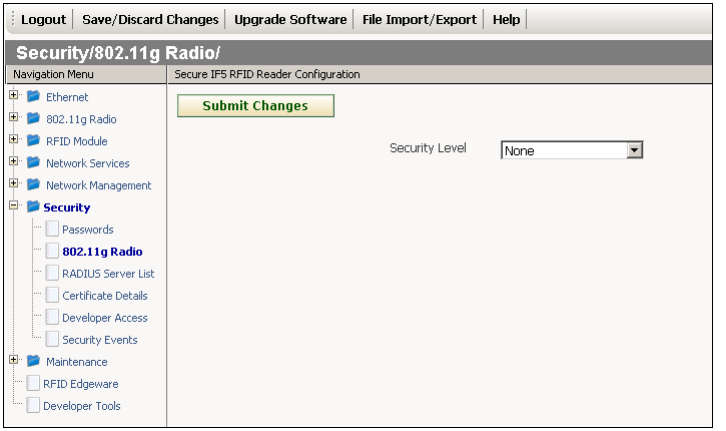
and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

Dynamic WEP Parameter Descriptions

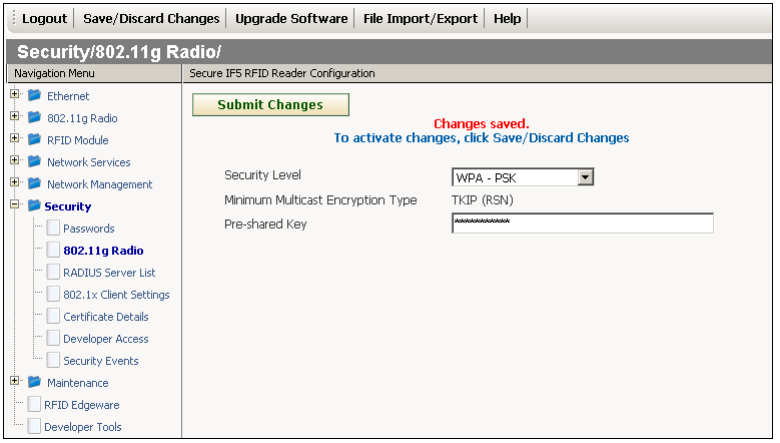
Parameter	Description
Authentication Method	Specifies whether encryption will be used as part of the authentication. Choose **Network EAP** to require encryption, or choose **Open System** to require no encryption.
Enable mixed cell	Enable this mode to allow the IF5 to communicate with Cisco access points configured for mixed-cell use. Mixed-cell use allows both WEP and non-WEP clients to communicate with the same access point.

Configuring WPA-PSK Security

1 From the menu, click **Security** > **802.11g Radio**. The Security/802.11g Radio screen appears.



2 Choose **WPA-PSK** from the **Security Level** drop-down list, and then click **Submit Changes**. This screen appears:

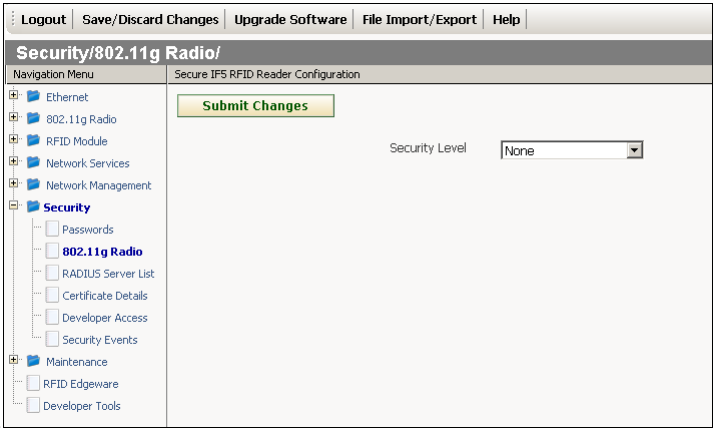


3 In the Pre-shared Key entry field, specify the pre-shared key for WPA.

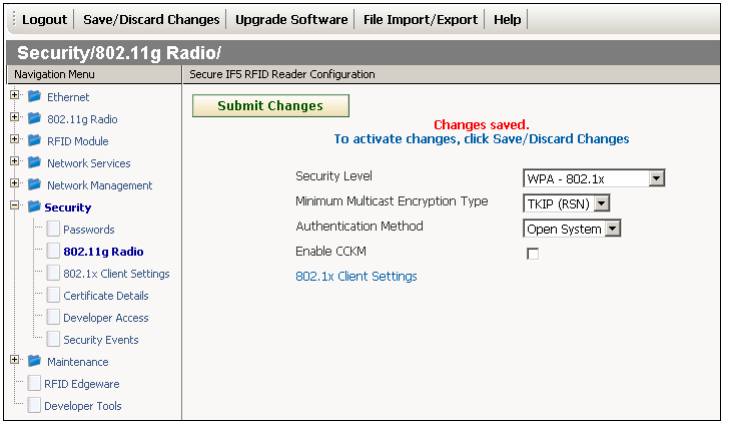
4 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

Configuring WPA-802.1x Security

1 From the menu, click **Security** > **802.11g Radio**. The Security/802.11g Radio screen appears.



2 Choose **WPA-802.1x** from the **Security Level** drop-down list, and click **Submit Changes**. This screen appears:



3 Configure the security parameters. For help, see the next table.

4 Click **802.1x Client Settings**. The Security/802.1x Client Settings screen appears.

5 Configure the 802.1x client settings. For help, see "Configuring 802.1x Client Settings" on page 60.

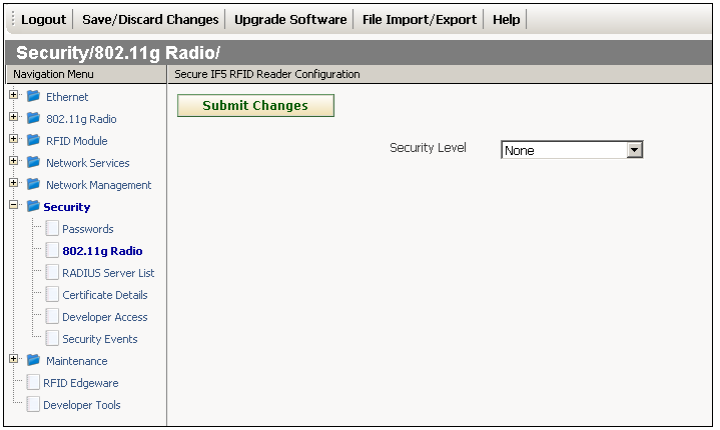
6 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

WPA-802.1x Parameter Descriptions

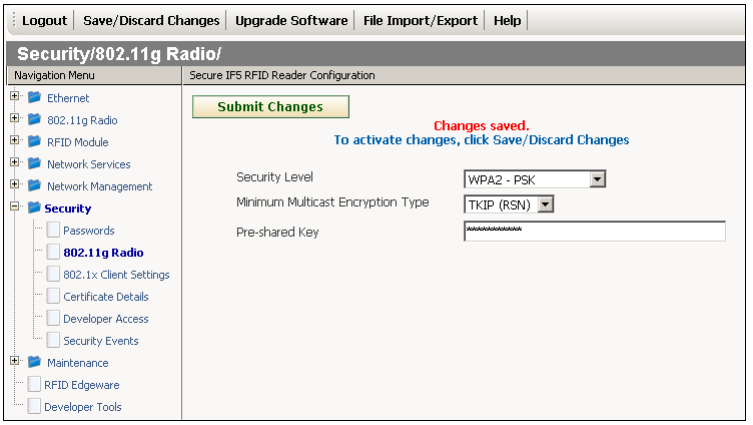
Parameter	Description
Minimum Multicast Encryption Type	Choose a data encryption method for non-unicast transmission/reception: **TKIP (RSN)**: Choose Temporal Key Integrity Protocol for multicast/group keying. **WEP (TSN)**: Choose WEP keying for multicast/group keying.
Authentication Method	Specifies whether encryption will be used as part of the authentication. Choose **Network EAP** to require encryption, or choose **Open System** to require no encryption.
Enable CCKM	Check this check box to enable fast roaming using Cisco's CCKM protocol.

Configuring WPA2-PSK Security

1 From the menu, click **Security** > **802.11g Radio**. The Security/802.11g Radio screen appears.



2 Choose **WPA2-PSK** from the **Security Level** drop-down list, and then click **Submit Changes**. This screen appears:



3 Configure the security parameters. For help, see the next table.

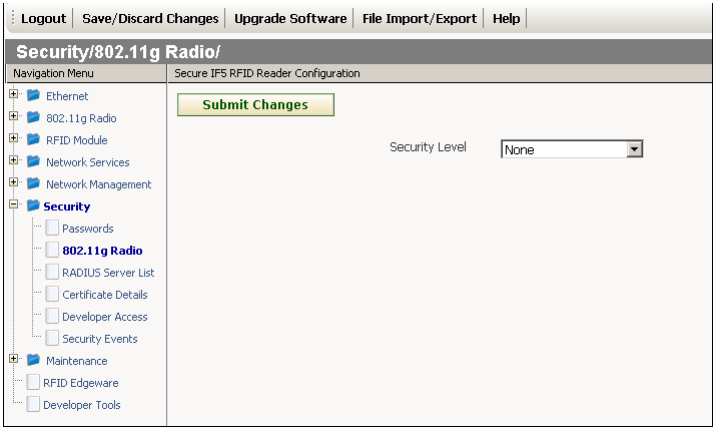
4 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

WPA2-PSK Parameter Descriptions

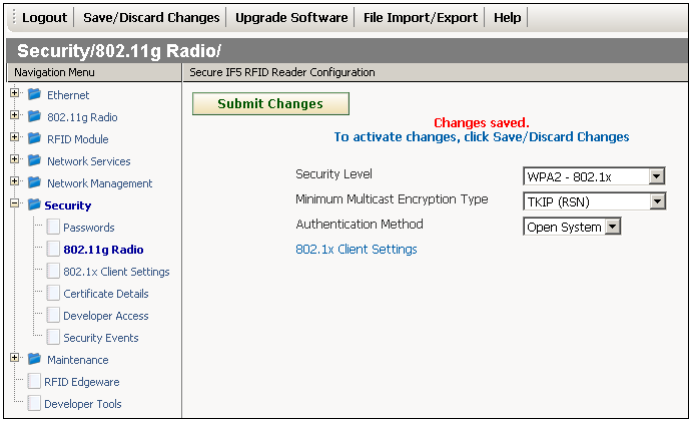
Parameter	Description
Minimum Multicast Encryption Type	Choose a data encryption method for non-unicast transmission/reception: **TKIP (RSN)** Use Temporal Key Integrity Protocol for multicast/group keying. **CCMP(TSN)**: Use Counter Mode - CBC MAC Protocol for multicast/group keying.
Pre-Shared Key	The pre-shared key for WPA. You can enter an ASCII passphrase, and the key will be derived from the passphrase using the PBKDF2 algorithm.

Configuring WPA2-802.1x Security

1 From the menu, click **Security** > **802.11g Radio**. The Security/802.11g Radio screen appears.



2 Choose **WPA2-802.1x** from the **Security Level** drop-down list, and click **Submit Changes**. This screen appears:



3 Configure the security parameters. For help, see the next table.

4 Click **802.1x Client Settings**. The Security/802.1x Client Settings screen appears.

5 Configure the 802.1x client settings. For help, see "Configuring 802.1x Client Settings" on page 60.

6 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

WPA2-802.1x Parameter Descriptions

Parameter	Description
Minimum Multicast Encryption Type	Choose a data encryption method for non-unicast transmission/reception: **CCMP (RSN)**: Use Counter Mode - CBC MAC Protocol for multicast/group keying. **TKIP (RSN)** (Temporal Key Integrity Protocol): Choose this option for multicast/group keying. **WEP (TSN, non-WiFi)** (Wired Equivalent Privacy): Choose this option to use WEP keying for group/multicast keys.
Authentication Method	Specifies whether encryption will be used as part of the authentication. Choose **Network EAP** to require encryption, or choose **Open System** to require no encryption.

Configuring 802.1x Client Settings

For Dynamic WEP and 802.1x security, you may need to configure 802.1x client settings. For help, see the next table.

802.1x Client Parameter Descriptions

Parameter	Description
Allow TLS	Enables/disables Transport Layer Security (TLS) authentication. If you enable TLS with WPA or 802.1x security, you must have a unique client certificate on the IF5 and a trusted root certificate authority (CA) certificate. For more information, see the next section, "About Certificates."
Allow TTLS (MSCHAPv2)	Enables/disables Tunneled Transport Layer Security (TTLS) authentication.
Allow PEAP	Enables/disables Protected Extensible Authentication Protocol (PEAP) authentication.
Allow LEAP	Enables/disables Lightweight Extensible Authentication Protocol (LEAP) authentication.

802.1x Client Parameter Descriptions (continued)

Parameter	Description
Preferred Protocol	Specifies which 802.1x authentication protocol (TLS, TTLS, PEAP, or LEAP) the IF5 sends to the authentication server if the server sends an unsupported protocol. If you do not allow an 802.1x authentication protocol, this parameter is not available.
User Name	User name for TTLS, PEAP, or LEAP authentication.
Password	Password for TTLS, PEAP, or LEAP authentication.
Verify CA Certificate	Enables/disables verification of the server certificate signature against the certificate installed on the IF5.

About Certificates

The default server certificate on the IF5 (ValidForHTTPSOnly) supports the secure web browser interface. If you choose to use transport layer security (TLS) with WPA-802.1x, WPA2-802.1x, or Dynamic WEP security, you need to have a unique client certificate on the IF5 and a trusted root certificate authority (CA) certificate. You can use a third-party CA to issue unique client certificates and a root certificate.

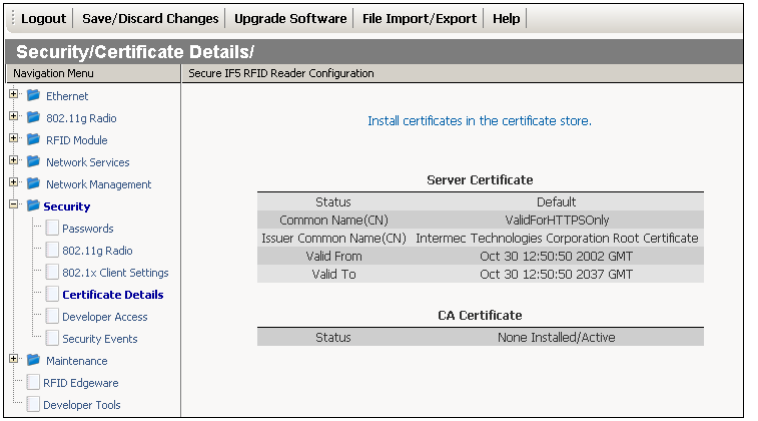
Note: To install or uninstall certificates, you need to access the IF5 via a secure web browser. For help, see "Using the Web Browser Interface" on page 19.

Viewing Certificates

You can use the web browser interface to view the certificates loaded on the IF5.

To view certificates

- From the menu, click **Security** > **Certificate Details**. The Certificate Details screen appears.



The Server Certificate table lists the server certificate that is installed, and the CA certificate table lists the trusted CA certificate that is installed.

Installing and Uninstalling Certificates

Once you have determined that you need to install or uninstall a certificate, use this procedure.

Note: If you follow the procedure to uninstall all certificates, you will lose the unique server certificate and the trusted CA certificate. You will need to contact your local Intermec representative to purchase new certificates.

Note: To install or uninstall certificates, you need to access the IF5 via a secure web browser. For help, see "Using the Web Browser Interface" on page 19.

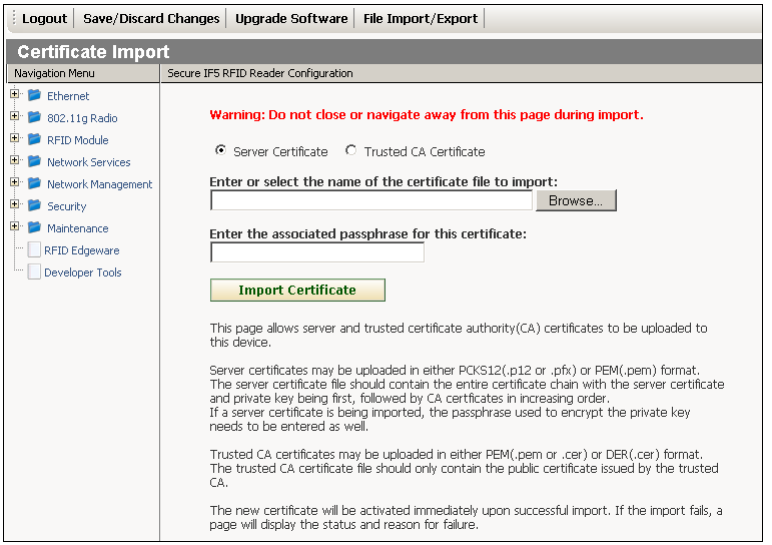
To install or uninstall certificates

1. From the main menu, click **Security** > **Certificate Details**. The Certificate Details screen appears.
2. To uninstall certificates, click **Uninstall all certificates**. The unique server certificate and the trusted CA certificate are deleted. You can still use the secure web browser interface and install new certificates using the default certificate (ValidForHTTPSOnly).

   To install certificates, continue with the next step.

3 Click **Install certificates in the certificate store**. The Certificate Import screen appears.

Note: If you are not using a secure web browser, you will be prompted to log in again. Click **A secure session is available** and log in to the IF5. If a Security Alert dialog box appears, click **Yes** to proceed. Repeat steps 1 through 3.


Logout
Save/Discard Changes
Upgrade Software
File Import/Export
Certificate Import
Navigation Menu
Secure IF5 RFID Reader Configuration
Ethernet
802.11g Radio
RFID Module
Network Services
Network Management
Security
Maintenance
RFID Edgeware
Developer Tools
Warning: Do not close or navigate away from this page during import.
Server Certificate
Trusted CA Certificate
Enter or select the name of the certificate file to import:
Browse...
Enter the associated passphrase for this certificate:
Import Certificate
This page allows server and trusted certificate authority(CA) certificates to be uploaded to this device.
Server certificates may be uploaded in either PCKS12(.p12 or .pfx) or PEM(.pem) format. The server certificate file should contain the entire certificate chain with the server certificate and private key being first, followed by CA certficates in increasing order.
If a server certificate is being imported, the passphrase used to encrypt the private key needs to be entered as well.
Trusted CA certificates may be uploaded in either PEM(.pem or .cer) or DER(.cer) format. The trusted CA certificate file should only contain the public certificate issued by the trusted CA.
The new certificate will be activated immediately upon successful import. If the import fails, a page will display the status and reason for failure.

4 Click **Server Certificate** or **Trusted CA Certificate**.

5 In the **Enter or select the name of the certificate file to import** field, enter the path to and filename of the server certificate. Or click **Browse** to find the certificate.

6 (Server Certificate only) In the **Enter the associated passphrase for this certificate** field, carefully enter the passphrase for the certificate.

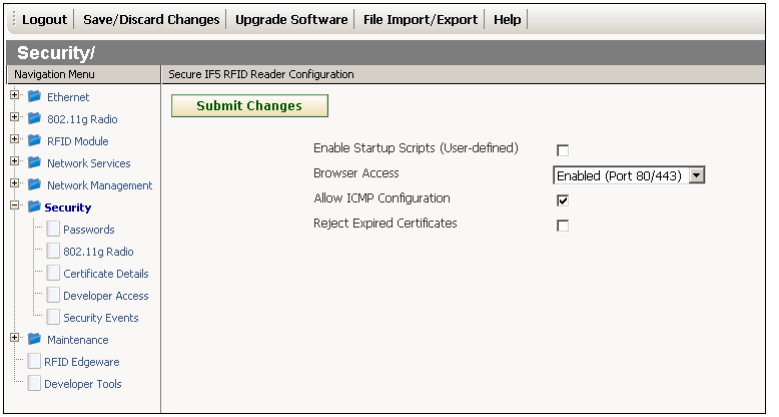
7 Click **Import Certificate**. If a Security Alert dialog box appears, click **Yes** to proceed.

Rejecting Expired Certificates

By default, when you install a certificate the IF5 does not validate the certificate dates against the date currently set in the IF5 operating system. Follow the next procedure to set the IF5 to reject expired certificates.

To set the IF5 to reject expired certificates

1 From the menu, click **Security**. The Security screen appears.



2 Check the **Reject Expired Certificates** check box.

3 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

3 Developing and Using RFID Applications

This chapter explains how you can develop and test RFID applications for the IF5 and includes these topics:

- RFID Applications and the IF5
- Creating RFID Applications for the IF5
- Running Applications at Boot Time
- About IF5 Edgeware
- About the IF5 RFID Architecture
- Configuring RFID Settings
- Configuring the Data Collection Engine
- Using the Diagnostics Tool
- Using the JavaScript Tool
- Configuring WEDM Settings (For IF5s with the IBM WRDI option only)

This chapter assumes you are familiar with developing applications and with your RFID system.

RFID Applications and the IF5

The IF5 supports Java RFID applications. Your application communicates with the IF5 through the Data Collection Engine (DCE), and controls the reader by issuing Basic Reader Interface (BRI) commands.

- For more information on the DCE, see "Configuring the Data Collection Engine" on page 80.
- For more information on the BRI, see the *Basic Reader Interface Programmer's Reference Manual* (P/N 937-000-xxx).

There are two ways to use the IF5 with your RFID application:

- You can run the application on a remote server. In this case, all processing is performed by the server.
- You can run the application locally on the IF5. In this case, the application resides on the IF5, and much of the processing occurs on the IF5 and not remotely on the server. Such an application is also known as edgeware, because the processing is done at the "edge" of the network.

Running your application as edgeware on the IF5 improves system scalability by minimizing network traffic, since the IF5 can handle many processing tasks such as data filtering.

If your application uses the IF5 GPIO interfaces to control external devices such as indicator lamps, running the application as edgeware decreases response time for those devices. For more information, see Chapter 5, "Using the IF5 GPIO Interfaces."

You can set up your application to auto-start when the IF5 boots. For more information, see "Running Applications at Boot Time" on page 70.

About the IBM WRDI Option

If you ordered the IBM WebSphere RFID Device Infrastructure (WRDI) option for the IF5, you need to enable the IF5 WEDM client so it starts at boot time. For help, see the next section.

After you enable the WEDM client, you can configure WEDM client settings using the web browser interface. For help, see "Configuring WEDM Settings" on page 95.

For more information, see the IBM WEDM documentation.

The Intermec-IBM WRDI SuperFeature CD (P/N 235-178-001) includes a set of plug-in components to IBM's WebSphere Studio Device Developer (WSDD) version 5.7.1. These include a sample WRDI application with the required driver bundles to support the IF5, as well as documentation about the sample and plug-in subsystems. For more information, contact your Intermec sales representative.

About the J2SE Option

If you ordered the Java J2SE option, the Java files are loaded at boot time. No further configuration is necessary. For more information, see the J2SE documentation.

Creating RFID Applications for the IF5

Intermec recommends this general outline for developing your RFID application:

1. Write and test your application on a development workstation (your desktop PC). The application can access the IF5 via TCP on port 2189.
2. After testing is complete, install the application on the IF5. You can package your application into a Java .jar file, and install the file and RFID Java libraries on the IF5 as appropriate. Be sure to specify the class path to the libraries. For help with executing Java applications, see "Executing Java Applications" on page 68.

Note: Java applications must be transferred to the IF5 as binaries, or errors will result.

To automatically run your application when the IF5 boots, see "Running Applications at Boot Time" on page 70.

Using the RFID Resource Kit

Intermec's RFID Resource Kit includes Java tools you can use to develop RFID applications that enable control of the reader and data management.

The resource kit is available as part of the Intermec Developer Library (IDL). To learn more about the IDL, go to www.intermec.com/idl.

Note: Previous versions of the IF5 firmware included the IDL RFID Java libraries. To minimize compatibility issues, the IF5 firmware no longer includes those libraries. You can obtain the libraries as part of the RFID Resource Kit download, and install them along with your application.

IF5 Java Support

The IF5 ships with IBM's WebSphere Everyplace MicroEnvironment (WEME). WEME implements the J2ME Connected Device Configuration (CDC)/Foundation 1.0 standard. The IF5 supports the CDC/Foundation profile, which is a subset of J2SE version 1.3.1.

The IF5 also comes with a SQL Server JDBC driver, located in /usr/local/jdbc. Use this driver to create applications that write data directly from the IF5 to a remote SQL Server database.

For more sophisticated Java development, the IF5 ships with the IBM Services Management Framework (SMF). This Java framework is an implementation of the open standard OSGi service-oriented architecture. This allows system administrators to install, uninstall, enable, and disable system services (also known as bundles) without having to reboot the IF5 each time. To use OSGi effectively, you need an OSGi server. For more information, see www.osgi.org.

Note: Because the IF5 Java runtime environment is based on J2ME CDC/Foundation 1.0, it does not support class files targeted for JDK 5 (or later) Virtual Machines. If you use a J2SE compiler to build your application, the generated class files must be compatible with JDK 1.4 VMs. Use `javac -source 1.4` to ensure class version compatibility.

Executing Java Applications

To execute a Java application on the IF5, use this command:

```
$JAVA_HOME/bin/j9 -jcl:foun10 MyJavaClass
```

To execute .jar files, use this command:

```
$JAVA_HOME/bin/j9 -jcl:foun10 -jar MyJar.jar
```

Note: Your .jar files must have manifest files included within them or the command will not work.

- The manifest needs to include an attribute called "Main-Class" to specify the application's entry point (for example, Main-Class: MyJavaClass).
- If the executable .jar needs to reference other .jar files, specify the files in the manifest file using the "Class-Path" attribute.

To enable the Java just-in-time (JIT) compiler for maximum performance, use this command:

```
$JAVA_HOME/bin/j9 -Xjit -jcl:foun10 -jar MyJar.jar
```

where:

`$JAVA_HOME` is an environment variable that indicates the Java runtime installation path. Always use this variable for simplicity and to insure that the correct runtime files are used.

`j9` is the name of the Java runtime executable installed in the IF5.

`-jcl:foun10` specifies that Foundation 1.0 classes should be used. To use additional class paths not defined in the Foundation 1.0 classes (such as components from the Intermec Developer Library), include the `-cp` option in the j9 parameters. Be sure to include the current path so classes in the current directory can be found, as shown in this example:

```
$JAVA_HOME/bin/j9 -jcl:foun10 -cp ./BasicRFID.jar:.MyClass
```

Note: Executing with JIT requires more memory. If your application uses large amounts of memory you may need to leave JIT disabled. JIT is disabled by default.

Java Support for Microsoft SQL Servers

The IF5 includes the jTDS JDBC Type 4 driver for connecting to Microsoft SQL Servers from Java applications. You need to include the location of the JDBC drivers in the class path. Use the environment variable $JDBC_HOME as shown in this example:

```
$JAVA_HOME/bin/j9 -jcl:foun10 -cp $JDBC_HOME/jtds-
j2me-1.0.2.jar:. MyClass
```

The only SQL server supported by the IF5 JDBC driver is the Microsoft SQL Server. For more information on the jTDS driver, go to http://jtds.sourceforge.net/doc.html.

IF5 JavaScript Support

The IF5 supports applications developed with JavaScript. Because JavaScript RFID applications can generally be written quickly, JavaScript is an ideal tool for creating demonstration software or proof-of-concept applications as well as production RFID edgeware.

You can configure the IF5 to auto-start a JavaScript application residing on the IF5 or on a remote server. The IF5 JavaScript implementation includes built-in objects that provide access to the BRI and the TCP, HTTP, SQL, and XML interfaces.

Running Applications at Boot Time

To run your Java RFID applications at boot time, you need to:

- enable startup scripts on the IF5.
- disable IF5 edgeware.
- copy your executables or scripts to the /home/developer/ startup directory on the IF5.

Follow the next procedure to set up the IF5 to run executables or scripts at boot time. For help with running a JavaScript file at boot time, see "Configuring a JavaScript File to Auto-Run at Boot Time" on page 92.

Note: Before you follow this procedure, Intermec recommends that you install your software on the IF5 and start it manually to verify that the executable or script runs properly.

To set up the IF5 to run executables or scripts at boot time

1. Enable startup scripts on the IF5. For help, see "Controlling Access to IF5 Menus" on page 42.
2. Enable FTP access to the IF5. For help, see "Controlling Developer Access" on page 44.
3. Disable edgeware on the IF5. For help, see the next section, "About IF5 Edgeware" on page 71.

4 Open an FTP connection to the IF5. When you connect to the IF5 via FTP, the /home/developer/ directory is the default location. For help, see "Using the FTP Server to Import and Export Files" on page 108.

5 Create a directory named "startup".

Note: If your IF5 has the Compact Flash option, you can also create the startup directory in the /cf/ directory.

6 Copy your executables or scripts via FTP to the startup directory.

7 (Optional) Disable FTP access to the IF5. FTP access to the IF5 is not required to run your software at boot time. For help with disabling FTP access, see "Controlling Developer Access" on page 44.

The IF5 is now ready to run the executable or script at boot time.

Handling Command Line Arguments at Boot Time

If your application does not require command line arguments, you can simply place the application into the startup directory as described in the previous section. Make sure your application is executable (chmod +x file).

If command line arguments or an exact startup order are necessary, use a shell script as shown in this example:

```
#!/bin/sh
/home/developer/other_apps/start_env
/home/developer/my_apps/testapp -D
```

About IF5 Edgeware

The IF5 comes with two types of installed edgeware:

- The Developer Tools, which include the Diagnostics tool and the JavaScript tool. The tools are enabled by default.

  Use the Diagnostics Tool to test and fine-tune your RFID systems and settings. For more information, see "Using the Diagnostics Tool" on page 84.

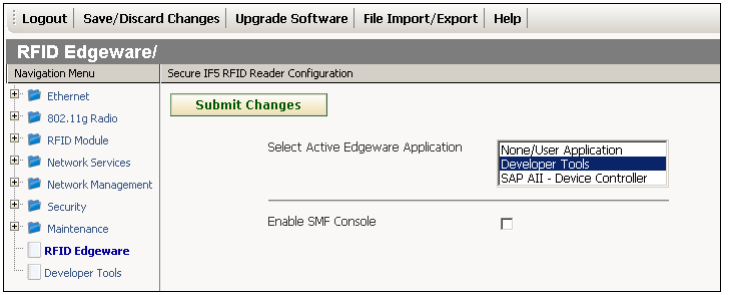
  Use the JavaScript Tool to edit and test JavaScript RFID applications. For more information, see "Using the JavaScript Tool" on page 90.

- The SAP device controller. Enable this edgeware so the controller communicates with the SAP backend module on your server. For more information, see "Enabling the SAP Device Controller" on page 140.

After you develop and test your RFID application, you can disable the internal edgeware to maximize IF5 resources for your application. For more information, see the next section.

To enable or disable RFID edgeware

1 From the menu, click **RFID Edgeware**. The RFID Edgeware screen appears.



2 Select one of the options in the list:

- Choose **None/User Application** to disable all IF5 edgeware. Choose this option if you want to load and run your own application on the IF5.
- Choose **Developer Tools** to use the IF5 developer tools for developing your own application.
- Choose **IBM WEDM + Developer Tools** if your IF5 includes the IBM WRDI software option. This option does not appear in the list if your IF5 does not include the WRDI option.
- Choose **SAP AII – Device Controller** to enable the SAP edgeware.

Note: To use the SAP edgeware, the SAP-AII backend module must be installed on your server. Contact your network administrator for more information.

3 (Optional) Check the **Enable SMF Console** check box if you want to enable the Service Management Framework console for remote interaction with the SMF framework.

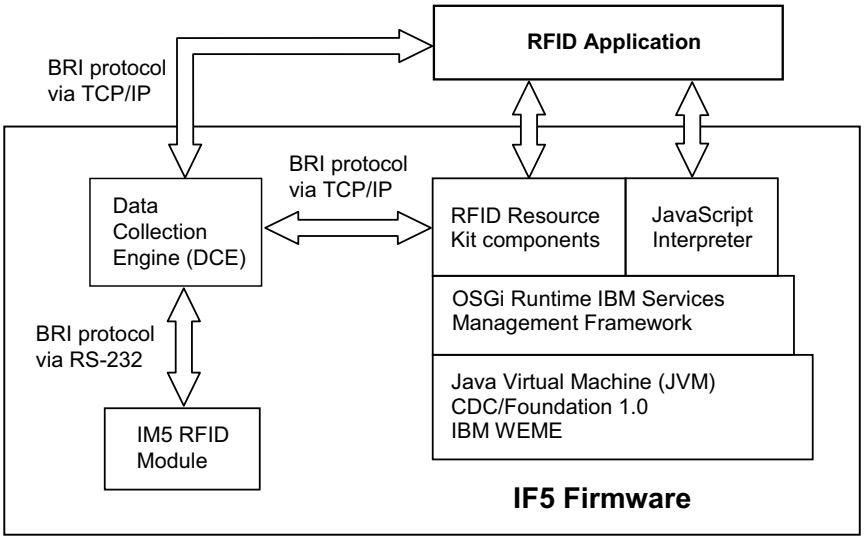
4 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

About the IF5 RFID Architecture

Your RFID application can communicate directly with the IF5 DCE using the BRI protocol. For more information, see "Configuring the Data Collection Engine" on page 80.

You can also use JavaScript applications with the IF5 RFID Resource Kit components to communicate with the DCE. For more information, see the RFID Resource Kit documentation.

The next illustration shows the basics of the IF5 RFID architecture.



IF5 RFID Architecture

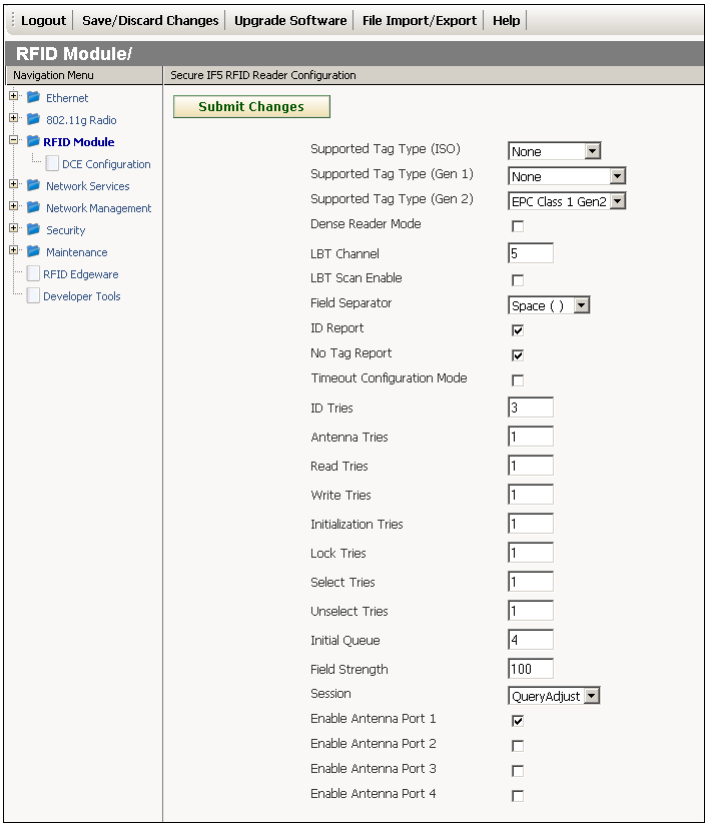
Configuring RFID Settings

This section explains how you use the web browser interface to change the settings for the IF5 RFID module. As you develop and test your application, you can configure the RFID settings for best system performance.

When you use the Diagnostics tool to display tags, the IF5 RFID module uses settings from the RFID Module screen. For help, see "Displaying Tags" on page 85.

To change RFID module settings

1 From the menu, click **RFID Module**. The RFID Module screen appears.



2 Change RFID settings as needed. For help, see the next section.

3 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

Note: If you make changes to RFID settings, you need to reboot the IF5 to activate the changes.

About RFID Module Settings

This section explains the module settings. Most settings have BRI attribute equivalents. For more information, see the *Basic Reader Interface Programmer's Reference Manual* (P/N 937-000-xxx).

Supported Tag Type (ISO)

Sets the type of ISO tag for RFID operations. See the next table for more information. Default is None.

This setting is equivalent to the TAGTYPE BRI attribute.

ISO Tag Type Descriptions

Tag Type	Description
ISO6B/G1	ISO6B Generation 1
ISO6B/G2	ISO6B Generation 2
Phillips v1.19	Phillips v1.19
None	Disables ISO tag operations

Supported Tag Type (Gen 1)

Enables or disables Gen 1 tag support for RFID operations. Choose **EPC Class 1 Gen 1** to enable Gen 1 support, or **None** (default) to disable Gen 1 support.

Supported Tag Type (Gen 2)

Enables or disables Gen 2 tag support for RFID operations. Choose **EPC Class 1 Gen 2** (default) to enable Gen 2 support, or **None** to disable Gen 2 support.

Dense Reader Mode

Check this check box to enable dense reader mode, which is only supported by EPC Class 1 Gen 2 tags. When dense reader mode is enabled, these tags respond with Miller Sub carrier encoded data instead of FM0 encoded data.

LBT Channel

(Supported only by 865 MHz readers) Sets the default transmit channel (of the 10 ETSI 302-208 channels) when the Listen Before Talk algorithm is enabled. Range is 1 to 10. Default channel is 5. This setting is used only when the LBT Scan Enable check box is not checked.

LBT Scan Enable

(Supported only by 865 MHz readers) Enables ETSI 302-208 channel scanning when the Listen Before Talk algorithm is enabled.

When this check box is checked, the LBT algorithm looks for a free transmit channel among the 10 available ETSI 302-208 channels. When this check box is not checked, the transmit channel is set by LBT Channel.

Field Separator

Sets the space character to be used for separating fields in tag data. Choose either space ( ) or comma (,). Default is space.

This setting is equivalent to the FIELDSEP BRI attribute.

ID Report

Enables or disables tag ID reporting after a Read, Write, or Lock command is executed:

- For ISO tags, the tag identifier corresponds to TAGID.
- For EPC tags, the identifier corresponds to EPCID.

Check the check box to enable tag ID reporting. This setting is equivalent to the IDREPORT BRI attribute, and is enabled by default.

No Tag Report

Enables or disables a NOTAG message, which is sent when no tags are found during execution of a Read, Write, or Lock command. Check the check box to enable the message. This setting is equivalent to the NOTAGRPT BRI attribute, and is enabled by default.

Timeout Configuration Mode

Enables a timeout mode. Instead specifying the number of antenna or ID tries, you specify a timeout value. If the IF5 does not find any tags after an antenna or ID try, the reader waits this long before starting the next antenna or ID try.

This setting is equivalent to the TIMEOUTMODE BRI attribute, and is disabled by default.

To enable Timeout Configuration mode

1. Check the check box and then click **Save Changes**. The screen refreshes. The Antenna Tries setting is replaced by Antenna Timeout, and the ID Tries setting is replaced by ID Timeout.
2. Specify the value (in ms) for the timeout in the entry fields and then click **Save Changes**.

ID Tries

Sets the maximum number of times the reader executes the identify algorithm before a response is returned to a Read or Write command.

In practice, this is the number of times a tag ID attempt is made for each antenna being used. Valid range is 1 to 254. Default is 3.

This setting is equivalent to the IDTRIES BRI attribute.

ID Timeout

Sets the ID timeout value (in ms) when Timeout Configuration mode is enabled. The maximum value is 65000 (default is 100). This setting is visible only if Timeout Configuration mode has been enabled. For help, see "Timeout Configuration Mode" in this section.

This setting is equivalent to the IDTIMEOUT BRI attribute.

Antenna Tries

Sets the maximum number of ID Tries that the reader executes per antenna. Valid range is 1 (default) to 254.

This setting is equivalent to the ANTTRIES BRI attribute.

Antenna Timeout

Sets the antenna timeout value (in ms) when Timeout Configuration mode is enabled. The maximum value is 65000 (default is 50). This setting is visible only if Timeout Configuration mode has been enabled. For help, see "Timeout Configuration Mode" in this section.

This setting is equivalent to the ANTTIMEOUT BRI attribute.

Read Tries
Sets the maximum number of times the read algorithm is executed before a response is returned to a Read command.

In practice, this is the number of times an identified tag will be read until the Read is successful. Valid range is 1 (default) to 254.

This setting is equivalent to the RDTRIES BRI attribute.

Write Tries
Sets the maximum number of times the write algorithm is executed before a response is returned to a Write command.

In practice, this is the number of times an identified tag will be written to until the Write is successful. Valid range is 1 (default) to 254.

This setting is equivalent to the WRTRIES BRI attribute.

Init Tries
Sets the maximum number of times the reader attempts to initialize a tag. Valid range is 1 (default) to 254.

This setting is equivalent to the INITTRIES BRI attribute.

Lock Tries
Sets the maximum number of times the lock algorithm is executed before a response is returned to a Lock command. Valid range is 1 (default) to 254.

This setting is equivalent to the LOCKTRIES BRI attribute.

Select Tries
(Not supported by EPCglobal Class 1 Gen 2 tags) Sets the number of times a group select is attempted. A group select is the command that starts the identity process. Valid range is 1 (default) to 254.

This setting is equivalent to the SELTRIES BRI attribute.

Unselect Tries
(Not supported by EPCglobal Class 1 Gen 2 tags) Sets the number of times a group unselect is attempted. Valid range is 1 (default) to 254.

Initial Queue

(EPCglobal Class 1 Gen 2 tags only) Sets the initial Q parameter value used by the Query command. Valid range is 0 to 15 (default is 4). If you know there is only one tag in the field, set this attribute to 0 for best performance.

This setting is equivalent to the INITIALQ BRI attribute.

Field Strength

Sets the RF power level (measured as a percentage of maximum power) for all antennas. Valid range is 0 to 100 (default is 100).

Use this setting to attenuate the antenna field strength. In some situations, full output power can cause unnecessary interference. For example, if the tag is close to the antenna, full output power might overload the tag and cause unreliable behavior.

This setting is equivalent to the FIELDSTRENGTH BRI attribute.

Session

(EPCglobal Class 1 Gen 2 tags only) Sets the command session parameter to the corresponding EPCglobal Class 1 Gen 2 air protocol command (default is QueryAdjust).

This setting is equivalent to the SESSION BRI attribute. For more information on this setting, see the EPCglobal Class 1 Gen 2 documentation.

Enable Antenna Port *n*

Enables or disables the antenna connected to antenna port *n*. Check the check box to enable that antenna. Antenna Port 1 is enabled by default.

If more than one antenna is enabled, the antennas always fire in sequence numerically (1, 2, 3, 4). To change this sequence, you need to set the ANTS BRI attribute. For more information, see the BRI programmer's reference manual.

Configuring the Data Collection Engine

The IF5 data collection engine (DCE) handles communication between your application and the RFID module, and allows up to 10 applications to use the same reader simultaneously.

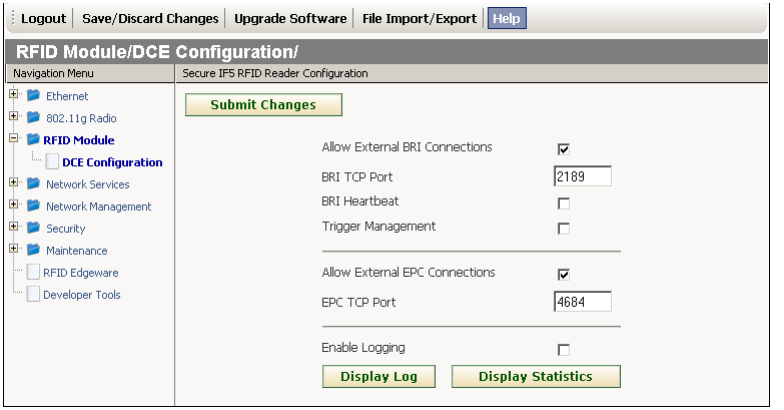
When your application is communicating with the DCE, the blue Intermec Ready-To-Work Indicator on the IF5 front panel turns on and stays on. For help, see "About the Intermec Ready-To-Work Indicator" on page 7.

You can configure many settings for the DCE. For help, see the next procedure.

Note: You need to disable the IF5 Developer Tools and the SAP device controller edgeware before your application can communicate with the DCE. For help, see "About IF5 Edgeware" on page 71.

To configure DCE settings

1 From the menu, click **RFID Module** > **DCE Configuration**. The DCE Configuration screen appears.



2 Change DCE settings as needed. For help, see the next table.

3 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

DCE Configuration Parameter Descriptions

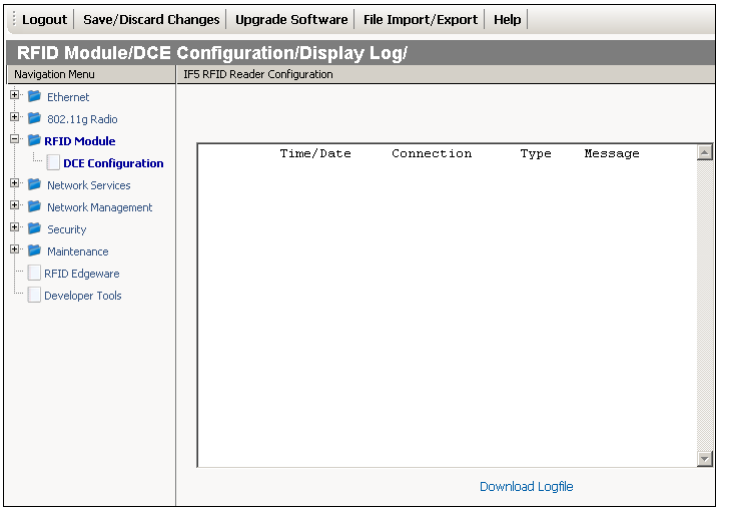
Parameter	Description
Allow External BRI Connections	Enables/disables external TCP connections to the DCE BRI server. If this check box is not checked, the DCE accepts BRI connections only from edgeware applications on the IF5.
BRI TCP Port	Specifies the TCP port used for incoming BRI connections to the DCE. This port must be unique for all TCP services running on the IF5. Valid range is 0 to 65535. Default is 2189.
BRI Heartbeat	Enables/disables an asynchronous heartbeat event (EVT: HEARTBEAT BRI STRING). When enabled, the IF5 sends the heartbeat event every 30 seconds, enhancing the IF5's ability to detect TCP sessions that were not closed cleanly.
Trigger Management	Enables DCE control of trigger states. When Trigger Management is enabled (default), the DCE manages the triggers so your application never needs to issue a TRIGGEREADY command. When Trigger Management is disabled, your application must manage issuance of the TRIGGERREADY command.
Allow External EPC Connections	Enables/disables external TCP connections to the DCE EPC server. When this box is not checked, the DCE accepts EPC connections only from applications residing on the IF5.
EPC TPC Port	Specifies the TCP port used for incoming EPC Reader Protocol connections to the DCE. This port number must be unique for all TCP services running on the IF5. Valid range is 0 to 65535 (default is 4684).
Enable Logging	Enables/disables logging of commands sent and received through the DCE.

Viewing the DCE Events Log

If you enable DCE logging, you can see a list of commands sent and received through the DCE. You can save the logfile as a .txt file.

To enable DCE logging and view the logfile

1. From the menu, click **RFID Module** > **DCE Configuration**. The DCE Configuration screen appears.
2. Check the **Enable Logging** check box.
3. Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.
4. After the IF5 reboots, click **Refresh** in the browser menu. The login screen appears.
5. Enter your user name and password, and then click **Login**. The TCP/IP Settings screen appears.
6. From the menu, click **RFID Module** > **DCE Configuration**. The DCE configuration screen appears.
7. Click **Display Log**. The DCE Configuration/Display Log screen appears with a list of command events. For more information on command events, see the next table.



8 To save the log file, click **Download Logfile** and then choose **File** > **Save As**. Follow the prompts to save the log file to your desktop PC.

DCE Log Command Event Descriptions

Event Name	Description
Time/Date	Time and date of the event.
Connection	TCP port of the event. 0 indicates a serial connection.
Type	Message type of the event, generally indicating which system sent the message: 0 - Message generated by the DCE for the logfile. 1 - Message from the RFID module to the DCE. 2 - Message from the DCE to the RFID module. 3 - Message from the application to the DCE. 4 - Message from the DCE to the application. Types 1 and 2 are suffixed by the message checksum value used by the reader module to detect errors.
Message	Text of the message, including responses.

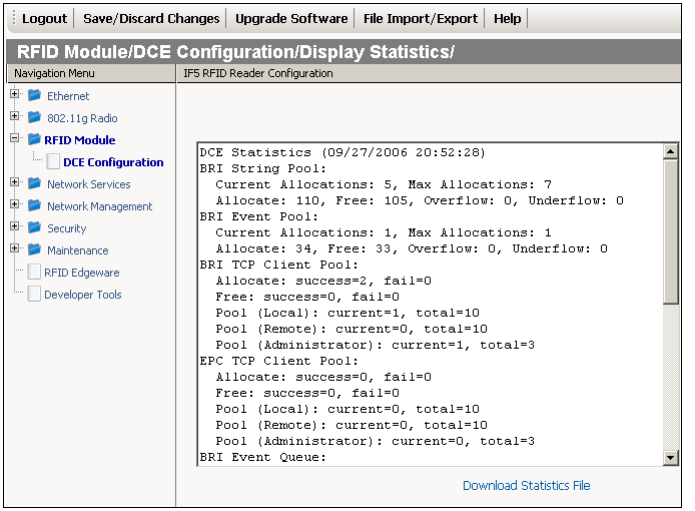
Viewing DCE Statistics

You can use the web browser interface to view a list of DCE statistics.

To view DCE statistics

1 From the menu, click **RFID Module** > **DCE Configuration**. The DCE Configuration screen appears.

2 Click **Display Statistics**. The DCE Configuration/Display Statistics screen appears with a list of DCE statistics.



3 To save the list, click **Download Statistics File** and then choose **File** > **Save As** in the browser menu. Follow the prompts to save the list to your desktop PC as a .txt file.

Using the Diagnostics Tool

You can use the Diagnostics tool to test and fine-tune your RFID system. The Diagnostics tool supports these features:

- Continuous tag reading, including tag ID reporting. For help, see the next section, “Displaying Tags.”
- General purpose input/output (GPIO) testing. For help, see “Testing the GPIO Interfaces” on page 86.
- Sending BRI commands or BRI script files to the IF5 from an interactive browser interface. For help, see “Using the BRI Window” on page 87.
- Running a tag read performance test. For help, see “Measuring Tag Read Performance” on page 88.

Note: To use the Diagnostics tool, you need to enable the IF5 Developer Tools. For help, see “About IF5 Edgeware” on page 71.

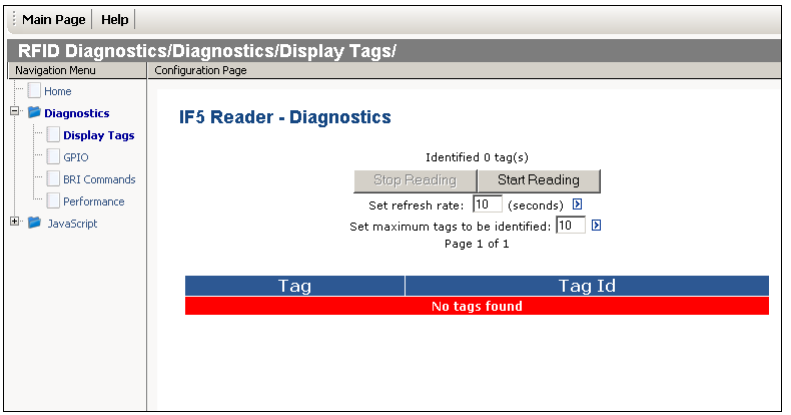
Displaying Tags

You can use the Diagnostics tool to continuously execute a read cycle on the IF5. For example, this procedure may be useful when you are testing antenna locations or tag placement.

Note: The read cycle is based on the settings listed in the RFID Module screen. For help, see "Configuring RFID Settings" on page 74.

To display tags and tag IDs

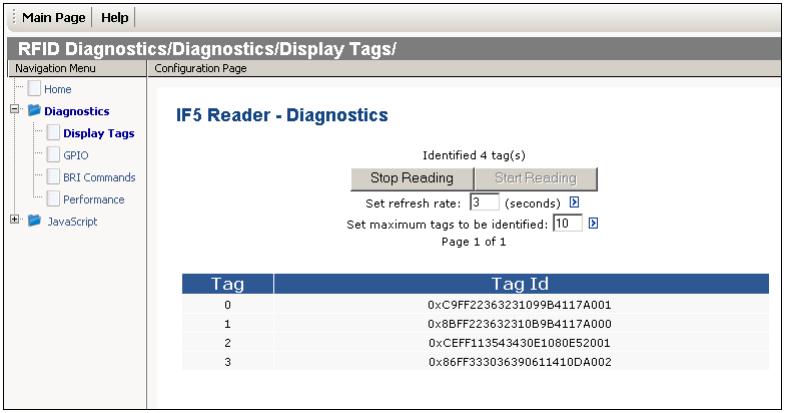
1 From the menu, click **Developer Tools**. The Display Tags screen appears.



- In the **Set refresh rate** entry field, enter the number of seconds for the read cycle, and then click ▶. The default is 10.
- In the **Set maximum tags to be identified** entry field, enter the maximum number of tags to identify during each read cycle, and then click ▶. The default is 10.

2 Click **Start Reading**. The IF5 looks for RFID tags within range of the connected antennas.

When the IF5 finds readable tags, the tag IDs appear in the list in the order in which they were read.



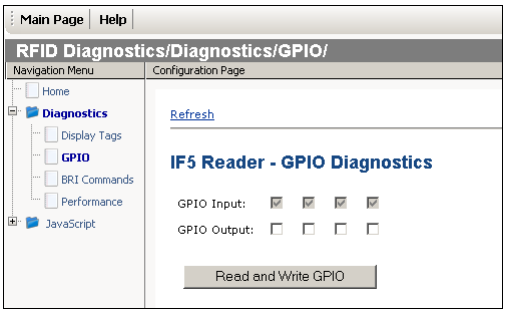
3 Click **Stop Reading** to end the read cycle.

Testing the GPIO Interfaces

If you have external GPIO controls such as motion sensors or indicator lamps connected to the IF5, you can use the Diagnostics tool to test the interfaces and verify that the controls behave as expected. Leave the controls connected to the IF5 control port when using the Diagnostics tool.

To test the GPIO interfaces

1 From the menu, click **Developer Tools** > **Diagnostics** > **GPIO**. The GPIO screen appears.



When this screen appears, the IF5 GPIO interfaces are turned off (equivalent to sending the BRI command `WRITEGPIO=0`).

The IF5 has four interfaces, numbered 1 to 4 from left to right on the screen.

2 Check the check box for each of the GPIO interfaces you want to test. When you check the check box, that GPIO output will be turned on (equivalent to `WRITEGPIO=15`), and its associated GPIO input is turned on.

   If a check box is not checked, that GPIO output is turned off and its associated GPIO input is turned off.

3 Click **Read and Write GPIO**. The GPIO interface state is changed.

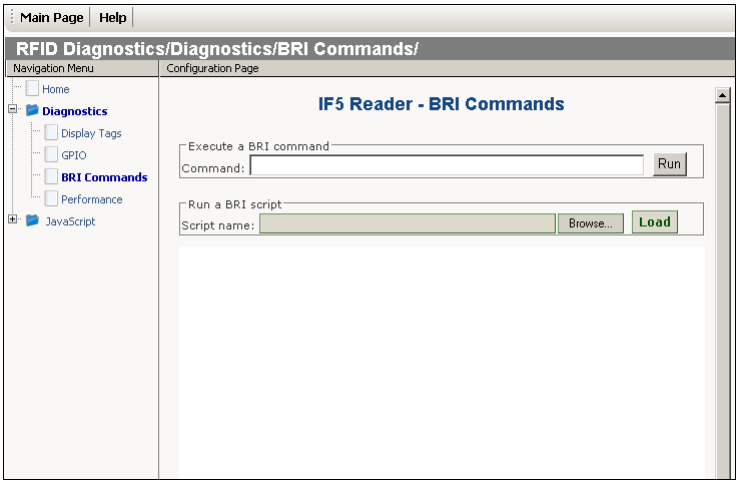
4 Click **Refresh** to show the current interface state.

Using the BRI Window

You can send BRI commands to the IF5 or load and run a BRI script through the web browser interface. For more information on BRI commands and syntax, see the BRI programmer's reference manual.

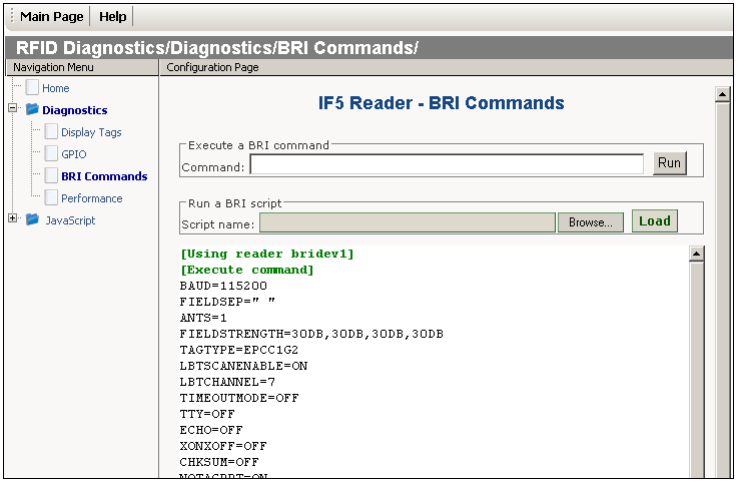
To send BRI commands

1 From the menu, click **Developer Tools** > **Diagnostics** > **BRI Commands**. The BRI Commands screen appears.



2 Enter the BRI command in the **Command** entry field.

3 Click **Run**. The command is executed and return values appear onscreen. For example, if you sent the ATTRIB command, the reader attributes appear in the list.



To load and run a BRI script

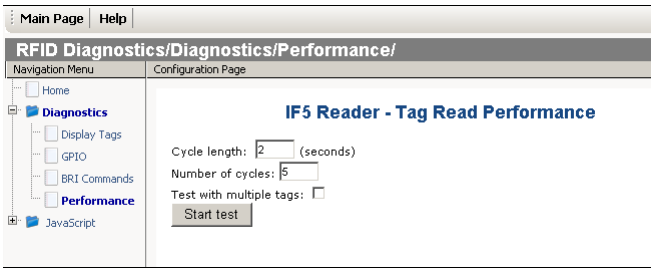
1. From the menu, click **Developer Tools** > **Diagnostics** > **BRI Commands**. The BRI Commands screen appears.
2. Click **Browse** and browse to the location of the BRI script.
3. Double-click the name of the file. The script filename appears in the **Script name** field.
4. Click **Load**. The script is loaded and run, and return values appear onscreen.

Measuring Tag Read Performance

You can run a tag read performance test to measure the efficiency of your RFID system. When you run the test, the IF5 executes a read cycle. You can configure the length (in seconds) of the cycle and the number of times the cycle is run.

To run a tag read performance test

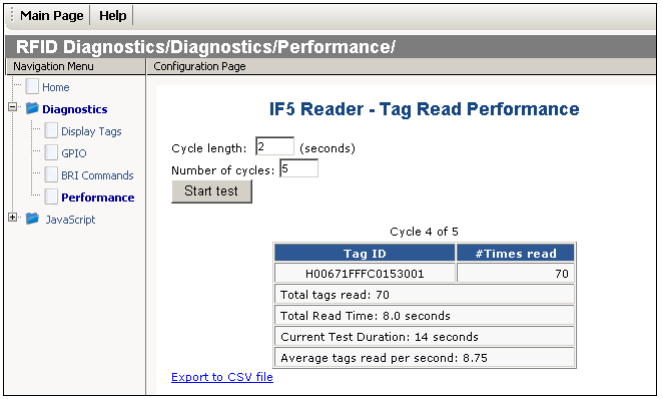
1. From the menu, click **Developer Tools** > **Diagnostics** > **Performance**. The Performance screen appears.



2 (Optional) Change settings for the performance test:

- Enter a value for the length of each read cycle in the **Cycle length** field. The default is two seconds.
- Enter a value for the number of read cycles in the **Number of Cycles** field. The default is five cycles.

3 Click **Start test**. The performance test begins and tag information appears in a table in the browser window.



The test returns this data:

- Tag ID: Tag ID for each identified tag. This field appears only if you have selected ISO6BG1 as the supported tag type.
- # Times read: Number of times each tag was read during the test. This field appears only if you have selected ISO6BG1 as the supported tag type.
- Total tags read: Total number of times all tags were read during the test

- Total Read Time: Elapsed time spent reading tags during the test
- Current Test Duration: Total time spent in the test cycle
- Average tags read per second: Total number of tags read divided by the total read time

4 To export the test results as a .csv file, click **Export to CSV file**. Follow the prompts to save the file.

About the Performance Test

When you click Start Test, the test cycle begins by setting the ANTTRIES, IDTRIES, INITTRIES, and RDTRIES reader attributes to 1. Then the test cycle executes the BRI command READ COUNT CONTINUOUS, sleeps for the amount of time specified by Cycle Length, executes READ POLL, and then executes a READ to end the continuous read cycle.

Using the JavaScript Tool

Note: These instructions assume you understand how to create and edit JavaScript files.

The JavaScript tool supports these functions:

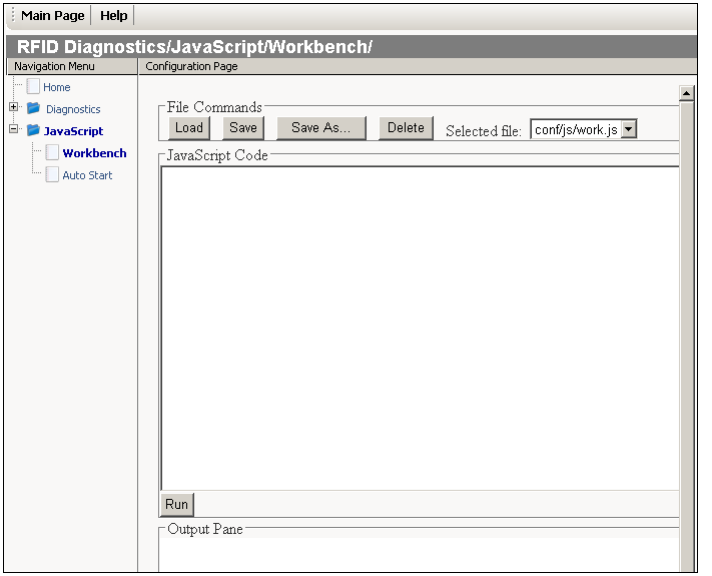
- Editing and sending JavaScript to the IF5 from the web browser interface. For help, see the next section, "Using the JavaScript Workbench."
- Configuring a JavaScript file to auto-run when the IF5 is rebooted. For help, see "Configuring a JavaScript File to Auto-Run at Boot Time" on page 92.

Using the JavaScript Workbench

You can create and edit a JavaScript file, load the file on the IF5, and run the file from the Workbench.

To create and run a JavaScript file

1 From the menu, click **Developer Tools** > **JavaScript** > **Workbench**. The Workbench screen appears.



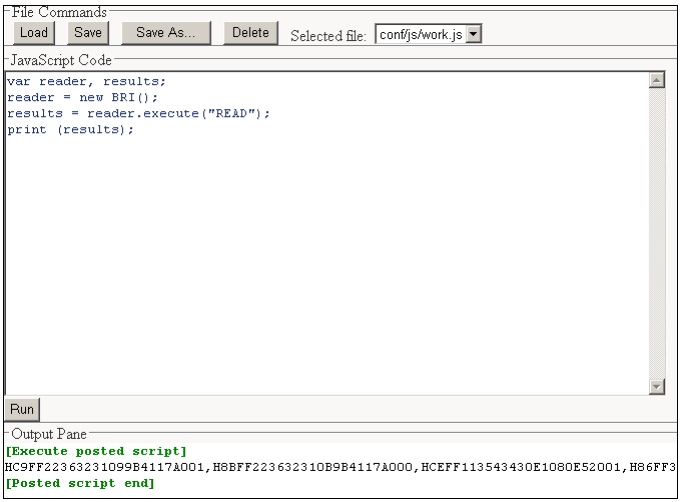
2 Click in the JavaScript Code box to enter code. You can also paste text copied from Notepad or another application. Copy the text from the other application and choose **Edit** > **Paste** in the browser menu.

3 To save your JavaScript code to the IF5 work buffer, click **Save**. The script is saved with the path and filename /conf/js/work.js.

To save your JavaScript to a different directory or with a different file name, click **Save As** and enter the new path and file name in the entry field. Click **OK**.

If you previously saved your JavaScript, click **Load** to reload it in the JavaScript Code box.

4 Click **Run**. The IF5 runs the JavaScript. Responses from the reader appear in the output pane. For example, if your script instructed the reader to read tags, the tag IDs appear in the Output Pane.



Configuring a JavaScript File to Auto-Run at Boot Time

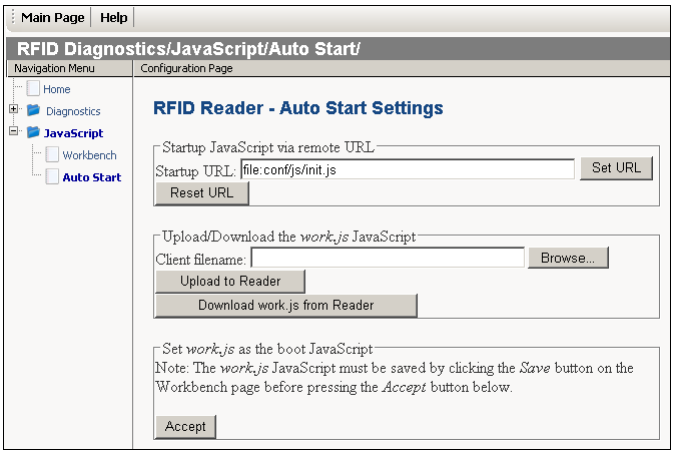
Note: For help with configuring the IF5 to run other executables or scripts when the IF5 boots, see "Running Applications at Boot Time" on page 70.

This section explains how to configure a JavaScript file to be automatically run when the IF5 is rebooted.

The startup file can be located on the IF5, or hosted on a remote server. When you set the file URL, a copy of the file is cached on the IF5 and executed if the server is unavailable at boot time.

To configure a JavaScript file to auto-run at boot time

1 From the menu, click **Developer Tools** > **JavaScript** > **Auto Start**. The Auto Start screen appears with the default startup path (file:conf/js/init.js) in the **Startup URL** field.



2 To specify a different startup file, enter the path to and name of the file in the **Startup URL** field.

- For a startup file that will reside on the IF5, use this format:

  `file:`*`mydirectory/myfilename.js`*

  where:

mydirectory	is the name of the directory on the IF5 where the file will be located.
myfilename.js	is the name of the file.

- For a startup file on a remote server, enter the URL as you would in a web browser's Address field, as in this example:

`http://www.mycompany.com/if5startup/`*`myfilename.js`*

3 Click **Set URL**. The file is configured to be the startup file. If the file is hosted remotely, a copy of the file is cached on the IF5 for use if the remote server is not available at boot time.

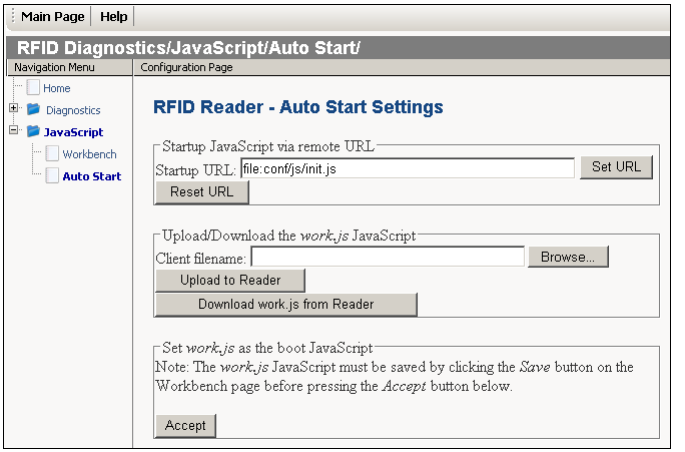
To reset the URL to the default (file:conf/js/init.js), click **Reset URL**.

Editing Remote Startup Files

To edit a remote startup file, you can upload the file from a remote server to the Workbench screen, where you can edit, test, and save your changes. You can also download the file from the IF5 to your desktop PC.

To edit a remote startup file

1 From the menu, click **Developer Tools** > **JavaScript** > **Auto Start**. The Auto Start screen appears.



2 Click **Browse** to browse to the startup file location, and double-click the file name. The path to and name of the file appear in the **Client filename** field.

3 Click **Upload to Reader**. The file is uploaded to the IF5.

4 In the left-hand pane, click **Workbench**. The Workbench screen appears.

5 Click **Load**. The file contents appear in the JavaScript Code box.

6 Edit the file. You can run the file to test it, and save it when you are finished editing. For help, see "Using the JavaScript Workbench" on page 91.

7 After you save the file, click **Auto Start** in the left-hand pane. The Auto Start screen appears.

8 To set the saved file as the startup file, click **Accept**.

To download the file from the IF5 to another location, click **Download work.js from Reader**. Follow the prompts to save the file.

Note: Before you can set the saved file as the startup file or download it from the reader, you need to save the file as described in Step 6.

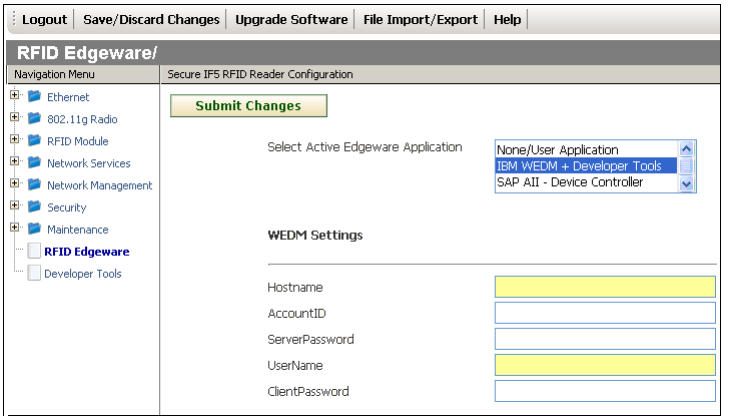
Configuring WEDM Settings

Note: This section only applies to IF5s ordered with the IBM WRDI option.

After you enable the WEDM client, you can use the web browser interface to configure settings. For help enabling the WEDM client, see "About IF5 Edgeware" on page 71.

To configure WEDM settings

1 From the menu, click RFID Edgeware. The RFID Edgeware screen appears with a list of configurable WEDM settings.



2 Change WEDM settings as needed. For more information, see the IBM WEDM documentation.

3 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

Note: When WRDI is active, some RFID module settings are changed from the default settings:

- Timeout Configuration Mode is enabled.
- Enable Antenna Port 2, 3, and 4 are enabled.
- Tag Type is set to EPCglobal Class 1 Gen 2.

4 Managing, Troubleshooting, and Upgrading the IF5

This chapter includes information on managing the IF5 and includes these topics:

- Managing the IF5
- Using Simple Network Management Protocol (SNMP)
- Using Wavelink Avalanche
- Using the Intermec SmartSystems Console
- Importing and Exporting Files
- Maintaining the IF5
- Troubleshooting the IF5
- Calling Intermec Product Support
- Upgrading Firmware

Managing the IF5

There are several methods you can use to manage the IF5. You can use:

- a web browser. For help, see "Using the Web Browser Interface" on page 19. This manual assumes you are using this method for all procedures.
- an SNMP management station. For help, see the next section.
- the Wavelink Avalanche client management system. For help, see "Using Wavelink Avalanche" on page 101.
- the Intermec SmartSystems Console. For help, see "Using the Intermec SmartSystems Console" on page 103.

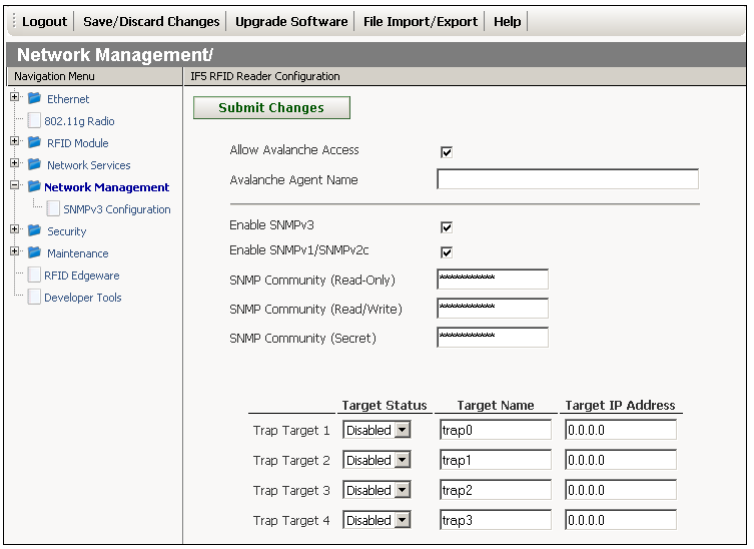
Using Simple Network Management Protocol (SNMP)

You can access and manage the IF5 from a Simple Management Network Protocol (SNMP) station. Contact your Intermec representative if you need to obtain a copy of the management information base (MIB).

Before you can use an SNMP management station, you must define the IF5 SNMP community strings.

To configure the SNMP community strings

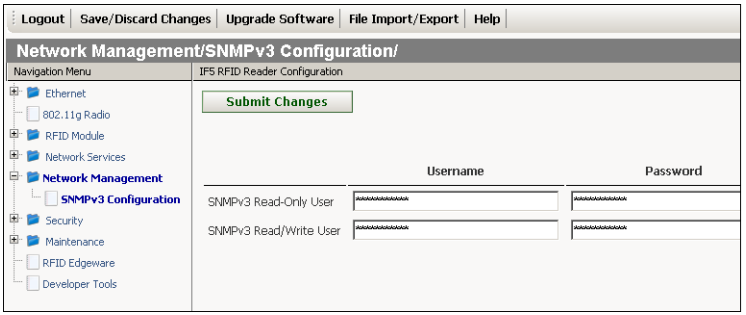
1 From the menu, click **Network Management**. The Network Management screen appears.



2 Configure the SNMP community parameters. For help, see the next table.

3 If you did not enable SNMPv3, continue with Step 5.

If you enabled SNMPv3, click **Network Management** > **SNMPv3 Configuration**. The SNMPv3 Configuration screen appears.



4 Change settings for SNMPv3. For help, see the next table.

5 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

SNMP Community Parameter Descriptions

Parameter	Description
Enable SNMPv3	Enables/disables SNMPv3.
Enable SNMPv1/ SNMPv2c	Enables/disables SNMPv1 and SNMPv2c.
SNMP Community (Read-Only)	Specifies a password that provides read-only access. This password can be from 1 to 15 characters and is case sensitive. The default is `public`.
SNMP Community (Read/Write)	Specifies a password that provides read and write access. This password can be from 1 to 15 characters and is case sensitive. The default is `CR52401`.
SNMP Community (Secret)	Specifies a password that provides read and write access and lets the user change the community strings. This password can be from 1 to 15 characters and is case sensitive. The default is `secret`.
SNMPv3 Read-Only User	Specifies a password that provides read-only access. This password can be from 1 to 15 characters and is case sensitive.
SNMPv3 Read-Write User	Specifies a password that provides read and write access. This password can be from 1 to 15 characters and is case sensitive.
Authentication Protocol	Specifies the protocol for authenticated SNMPv3 messages. This must match a supported authentication protocol on the SNMP management station.
Data Privacy Protocol	Specifies the protocol for encrypted SNMPv3 messages. This must match a supported encryption protocol on the SNMP management station.

Using Wavelink Avalanche

The Wavelink Avalanche client management system uses three main components to help you easily manage your wireless network.

Avalanche Component Descriptions

Component	Description
Enabler	Resides on all devices that can be managed by the Avalanche system. It communicates information about the device to the Avalanche Agent and manages software applications on the device.
Agent	Automatically detects and upgrades all devices in the Avalanche system and manages the daily processing functions.
Console	The administrative user interface that lets you configure and communicate with the Avalanche Agent. From the console, you can configure and monitor devices and build and install software packages and software collections.

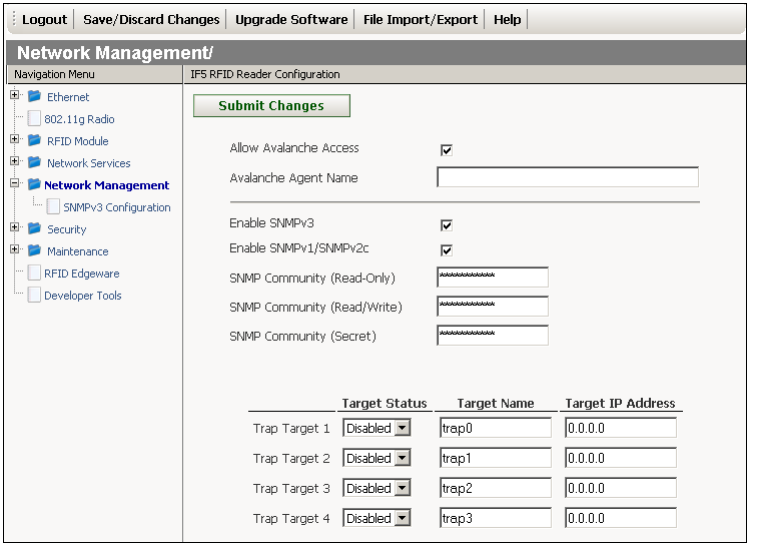
The enabler is already installed on IF5s with firmware release 2.0 and later. Avalanche uses a hierarchical file system organized into software packages and software collections:

- Software packages are groups of files for an application that resides on the device.
- Software collections are logical groups of software packages.

For more information, see the Wavelink Avalanche documentation and online help. Or, visit the Wavelink web site at www.wavelink.com.

To configure the IF5 to use Avalanche

1 From the menu, click **Network Management**. The Network Management screen appears.



2 Configure Avalanche settings. For help, see the next table.

3 Click **Submit Changes** to save your changes. To activate your changes, from the menu bar click **Save/Discard Changes**, and then click **Save Changes and Reboot**. For help, see "Saving Configuration Changes" on page 22.

Wavelink Avalanche Parameter Descriptions

Parameter	Description
Allow Avalanche Access	Enables/disables the Avalanche client management system.
Avalanche Agent Name	Specifies the IP address or DNS name of the Avalanche console. Or, leave this field blank and the IF5 sends out a broadcast request looking for any available agent.

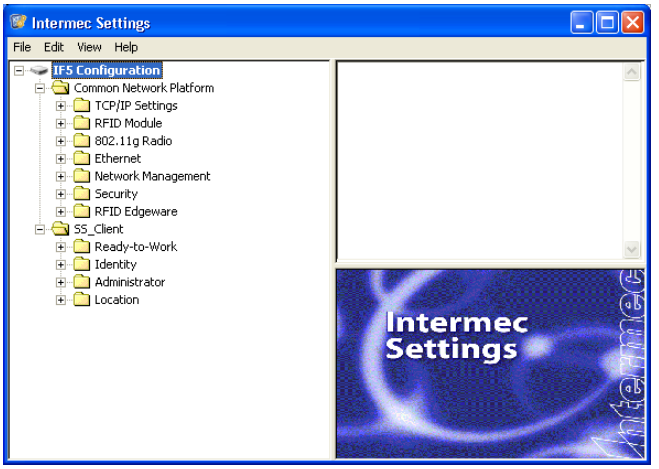
Using the Intermec SmartSystems Console

The IF5 ships with a SmartSystems Client, which means you can manage it from a central host PC using Intermec's SmartSystems Foundation. The SmartSystems Console displays all SmartSystems-enabled devices in your network.

The SmartSystems Foundation is available for free from the Intermec web site. To download SmartSystems Foundation, go to www.intermec.com/SmartSystems. For information on using the SmartSystems Console, in the Console choose **SmartSystems** > **Help**.

Configuring the IF5 with Intermec Settings

In the Console, right-click an IF5 and choose **Intermec Settings** from the menu. The Intermec Settings browser appears.



Intermec Settings: *If you use the SmartSystems Console to manage the IF5, you can use Intermec Settings to configure the IF5.*

For help with using Intermec Settings, in the Intermec Settings browser choose **Help** > **Online Manual**.

Importing and Exporting Files

This section explains how to move files between the IF5 and your desktop PC.

Note: Do not use this procedure to copy upgrade files to the IF5. For help with upgrades, see "Upgrading Firmware" on page 123.

To move files between the IF5 and your desktop PC, you can:

- use the web browser interface. For help, see the next section, "Using the Web Browser to Import and Export Files."
- use the IF5 FTP server. For help, see "Using the FTP Server to Import and Export Files" on page 108.
- auto-mount a Network File System (NFS) share at boot time. For help, see "Controlling Developer Access" on page 44.

Using the Web Browser to Import and Export Files

You can use the web browser to move files to and from the IF5, and to browse the IF5 directories.

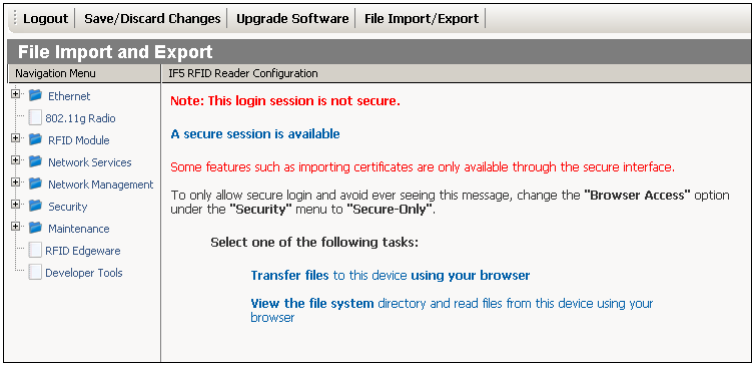
Browsing the IF5 and Importing Files to Your PC

This section explains how to use the web browser interface to browse directories and import files from the IF5 to your PC.

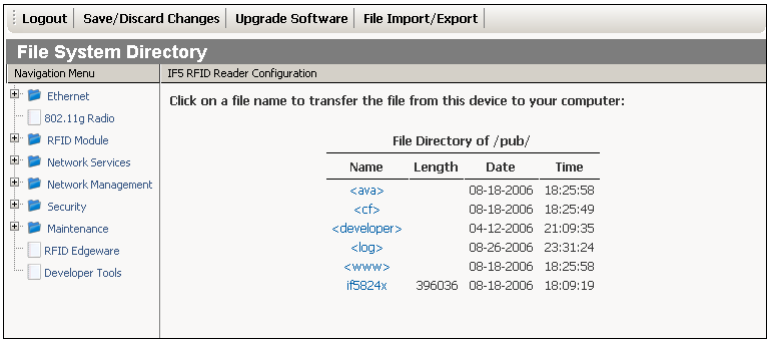
You can also use the JavaScript Auto Start tool to import startup script files to the IF5. For help, see "Using the JavaScript Tool" on page 90.

To browse the IF5 directories

1 From the menu, click **File Import/Export**. The File Import and Export screen appears.


Logout
Save/Discard Changes
Upgrade Software
File Import/Export
File Import and Export
Navigation Menu
IF5 RFID Reader Configuration
Ethernet
802.11g Radio
RFID Module
Network Services
Network Management
Security
Maintenance
RFID Edgeware
Developer Tools
Note: This login session is not secure.
A secure session is available
Some features such as importing certificates are only available through the secure interface.
To only allow secure login and avoid ever seeing this message, change the "Browser Access" option under the "Security" menu to "Secure-Only".
Select one of the following tasks:
Transfer files to this device using your browser
View the file system directory and read files from this device using your browser

2 Click **View the file system directory and read files from this device using your browser**. The File System Directory screen appears, showing the contents of the /home/intermec/pub directory.

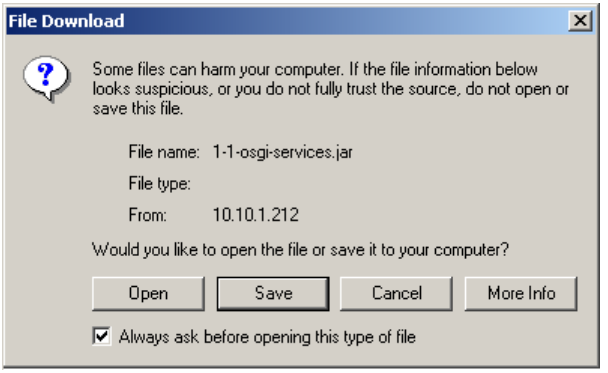


3 In the File System Directory screen, you can:

- click <*directory*> to browse that directory.
- click <..> to return to the previous directory.
- click a filename to view or download that file.

Text files, XML files, and other user-readable files can be viewed in the browser window. To copy a viewable file to your desktop PC, choose **File** > **Save As** in the browser window and follow the prompts to save the file to your desktop PC.

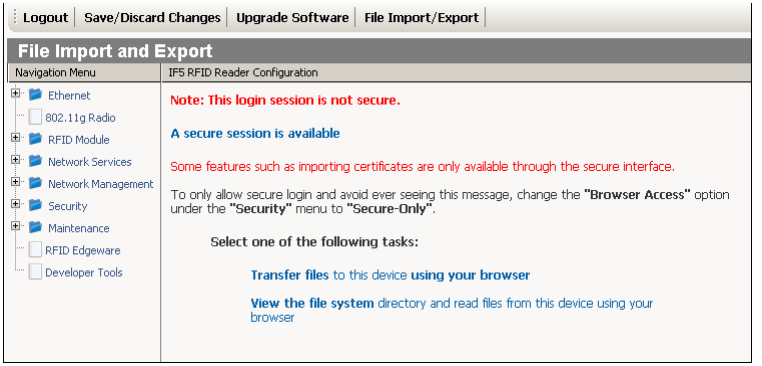
If a file cannot be viewed in the browser, a File Download message appears.


File Download
Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.
File name: 1-1-osgi-services.jar
File type:
From: 10.10.1.212
Would you like to open the file or save it to your computer?
Open
Save
Cancel
More Info
Always ask before opening this type of file

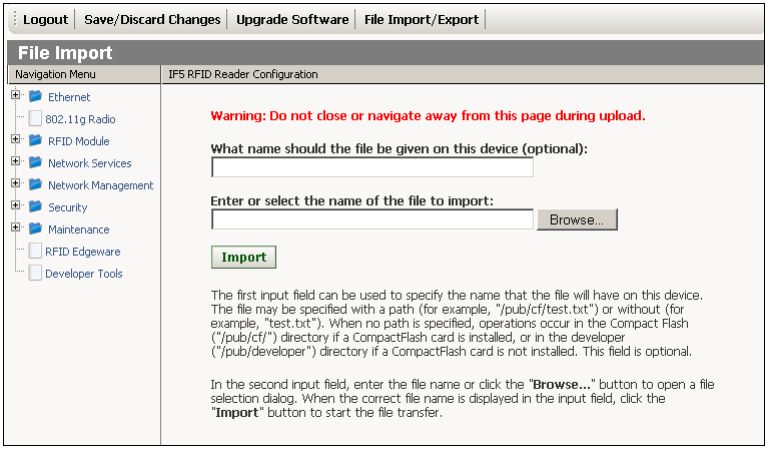
Follow the prompts to copy the file from the IF5 to your desktop PC.

Importing Files to the IF5

1 From the menu, click **File Import/Export**. The File Import and Export screen appears.


Logout
Save/Discard Changes
Upgrade Software
File Import/Export
File Import and Export
Navigation Menu
IF5 RFID Reader Configuration
Ethernet
802.11g Radio
RFID Module
Network Services
Network Management
Security
Maintenance
RFID Edgeware
Developer Tools
Note: This login session is not secure.
A secure session is available
Some features such as importing certificates are only available through the secure interface.
To only allow secure login and avoid ever seeing this message, change the "Browser Access" option under the "Security" menu to "Secure-Only".
Select one of the following tasks:
Transfer files to this device using your browser
View the file system directory and read files from this device using your browser

2 Click **Transfer files to this device using your browser**. The File Import screen appears.


Logout
Save/Discard Changes
Upgrade Software
File Import/Export
File Import
Navigation Menu
IF5 RFID Reader Configuration
Ethernet
802.11g Radio
RFID Module
Network Services
Network Management
Security
Maintenance
RFID Edgeware
Developer Tools
Warning: Do not close or navigate away from this page during upload.
What name should the file be given on this device (optional):
Enter or select the name of the file to import:
Browse...
Import
The first input field can be used to specify the name that the file will have on this device. The file may be specified with a path (for example, "/pub/cf/test.txt") or without (for example, "test.txt"). When no path is specified, operations occur in the Compact Flash ("/pub/cf") directory if a CompactFlash card is installed, or in the developer ("/pub/developer") directory if a CompactFlash card is not installed. This field is optional.
In the second input field, enter the file name or click the "Browse..." button to open a file selection dialog. When the correct file name is displayed in the input field, click the "Import" button to start the file transfer.

3 Click **Browse** to browse to the location of the file to be imported, and double-click the filename. The name of the file appears in the **Enter or select the name of the file to import** entry field.

4 (Optional) In the **What name should the file be given on this device (optional)** entry field, enter the path to and new filename for the file that will be imported to the IF5.

- If your IF5 includes the Compact Flash memory option, leave this field blank to import the file to the /pub/cf directory with its original filename.
- If your IF5 does not include the Compact Flash memory option, leave this field blank to import the file to the /pub/developer directory with its original filename.

5 Click **Import**. The file is imported to the IF5.

Using the FTP Server to Import and Export Files

You can move files to and from the IF5 by using its resident FTP server. The IF5 FTP server is disabled by default. To enable the FTP server, see "Controlling Developer Access" on page 44.

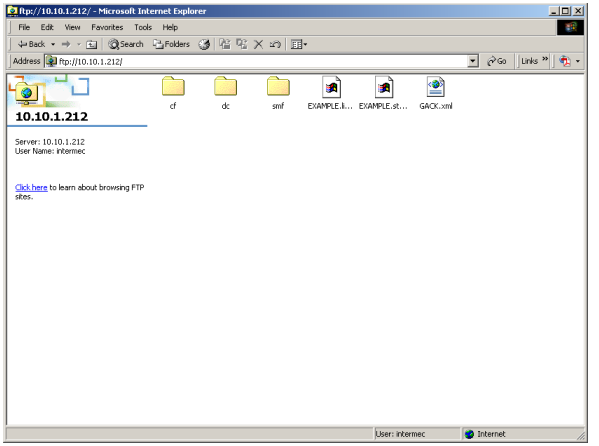
After you enable the IF5 FTP server, you can access the FTP directory directly through Internet Explorer, or from the IF5 web browser interface. As with any Windows directory, you can click-and-drag or copy-and-paste to move files.

To access the FTP directory directly

1. Open Internet Explorer.
2. In the **Address** field, enter this text:

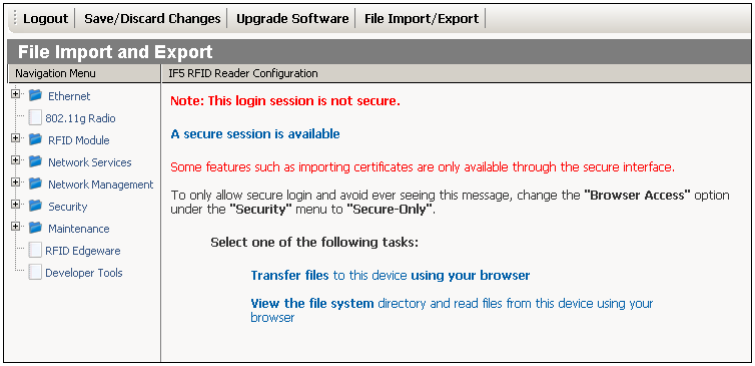
   ftp:*xxx.xxx.xxx.xxx*

   where *xxx.xxx.xxx.xxx* is the IF5 IP address.
3. Press **Enter**. The **Login As** dialog box appears.
4. Type `intermec` in the **User Name** and **Password** fields, and then click **Login**. The IF5 FTP directory appears.

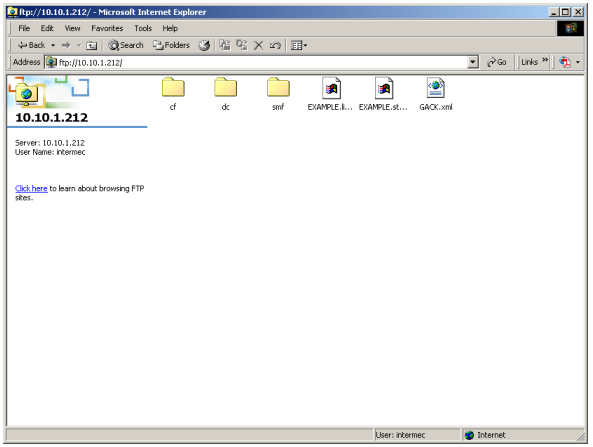


To access the FTP directory from the IF5 web browser interface

1 In the web browser interface, click **File Import/Export**. The File Import and Export screen appears.


Logout
Save/Discard Changes
Upgrade Software
File Import/Export
File Import and Export
Navigation Menu
IF5 RFID Reader Configuration
Ethernet
802.11g Radio
RFID Module
Network Services
Network Management
Security
Maintenance
RFID Edgeware
Developer Tools
Note: This login session is not secure.
A secure session is available
Some features such as importing certificates are only available through the secure interface.
To only allow secure login and avoid ever seeing this message, change the "Browser Access" option under the "Security" menu to "Secure-Only".
Select one of the following tasks:
Transfer files to this device using your browser
View the file system directory and read files from this device using your browser

2 Click **Transfer files to or from this device using FTP**. The IF5 FTP directory appears in a new browser window.



Maintaining the IF5

The Maintenance menu lets you view IF5 parameters and statistics, including:

- connections to access points (for wireless networks).
- access point neighbors (for wireless networks).
- port statistics.
- a list of logged events.
- a configuration summary.

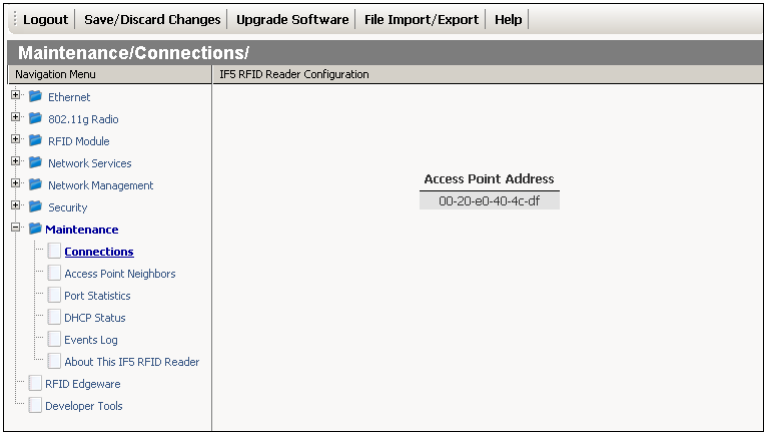
You may need this information when you call Intermec Product Support.

Viewing Connections

The Connections screen shows the access point MAC address. You can see the Connections screen only if the 802.11g radio is active and connected to an access point.

To view connections

- From the menu, click **Maintenance**. The Connections screen appears. This screen is read-only.



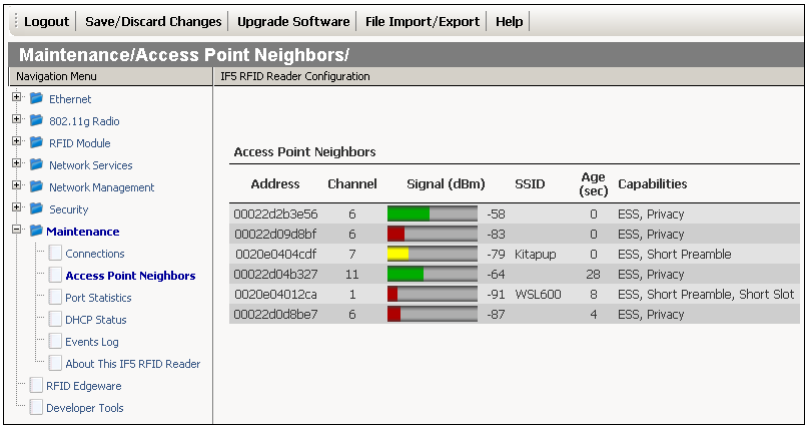
Viewing Access Point Neighbors

The AP Neighbors screen provides information on all the access points (even hidden access points) in the area. This screen shows information gathered by the radio receiving beacons from other sources as it operates on a specific channel. You can use this screen to help you:

- distribute channels for maximum wireless network performance.
- identify interference problems.

To view AP neighbors

- From the menu, click **Maintenance** > **AP Neighbors**. The AP Neighbors screen appears. For help interpreting the information on this read-only screen, see the next table.



AP Neighbors Screen Fields

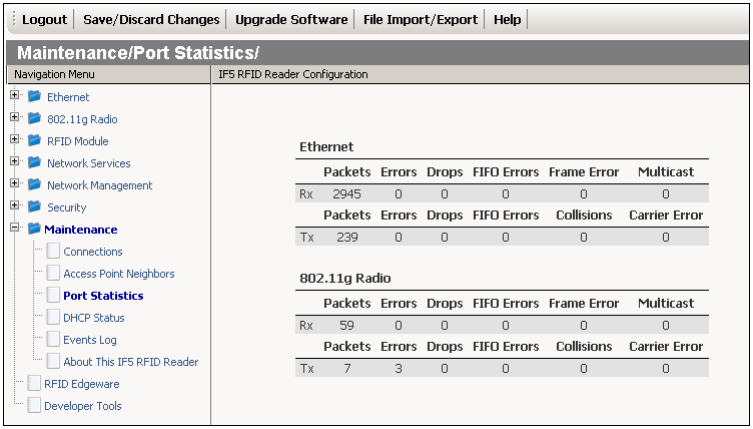
Field	Description
Address	Displays the MAC address of the access point.
Channel	Shows the channel advertised in the beacon.
Signal(dBm)	Indicates power level of reception measured in dBm. The colors red, yellow, and green indicate poor, adequate, and good signal levels, respectively.
SSID	Displays the SSID advertised in the beacon. This field may or may not be advertised by the originator of the contact.
Age (sec)	Shows the amount of elapsed time since the last contact from the originator.
Capabilities	Displays information derived from the capability information sent in the beacon, which may include: **ESS:** Set for an access point and cleared for an end device or ad-hoc device. **IBSS:** Cleared for an access point and set for an end device or ad-hoc device. **Privacy:** Indicates that encryption is required on this service set. **Short Preamble:** Indicates that short preambles may be used for frame transmission on this service set. **OFDM Allowed:** DSSS-OFDM is allowed on this service set. **Short Slot:** Short slots timing is being used on this service set. If this field is not present, longer slot timing is being used for backward compatibility. **CFPoll:** Access point uses coordination function for delivery and polling. **CFReq:** Access point uses point coordination function for delivery but does not support polling.

Viewing Port Statistics

The Port Statistics screen shows the total number of frames and bytes that the IF5 has received and transmitted since it was last booted.

To view port statistics

- From the menu, click **Maintenance** > **Port Statistics**. The Port Statistics screen appears. This screen is read-only.

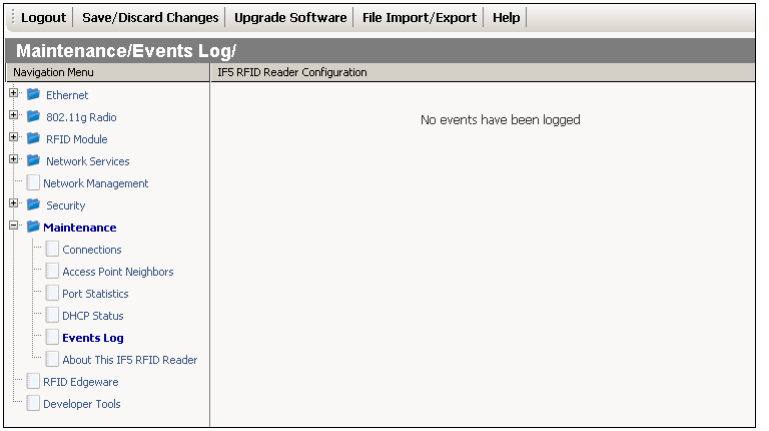


Viewing the Events Log

The Events Log screen shows events that have been logged by the IF5. These events are cleared when the IF5 loses power or is rebooted.

To view the Events screen

- From the menu, click **Maintenance** > **Events Log**. The Events Log screen appears. This screen is read-only.

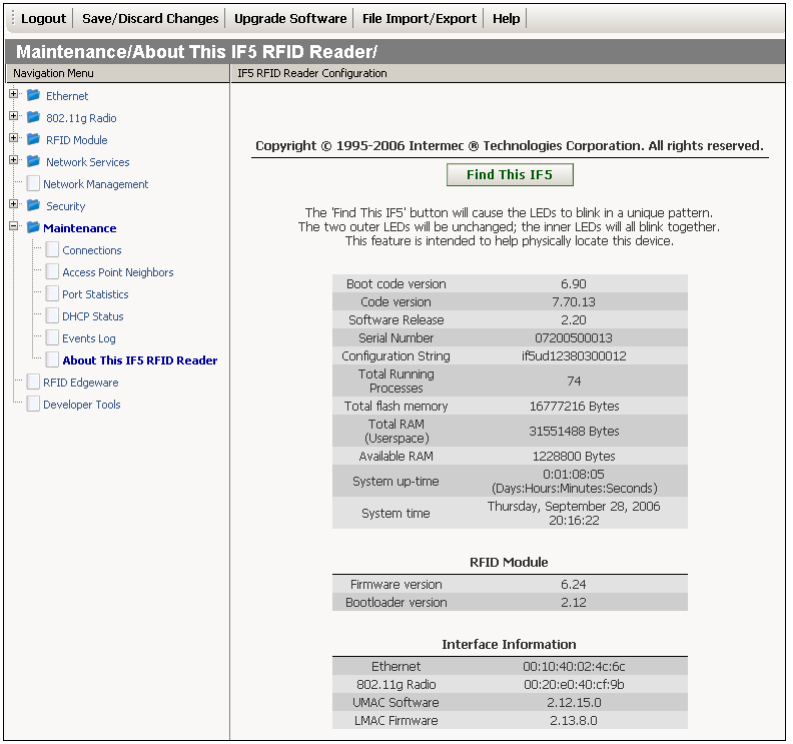


Viewing the About This IF5 RFID Reader Screen

The About This IF5 RFID Reader screen summarizes the configuration settings for the IF5 and includes a list of software versions, serial numbers, and other IF5-specific information. Any changes from the default configuration that have been made to this IF5 appear as blue.

To view the About This IF5 screen

- From the menu, click **Maintenance** > **About This IF5 RFID Reader**. The About This IF5 RFID Reader screen appears. This screen is read-only.



Using the LEDs to Locate the IF5

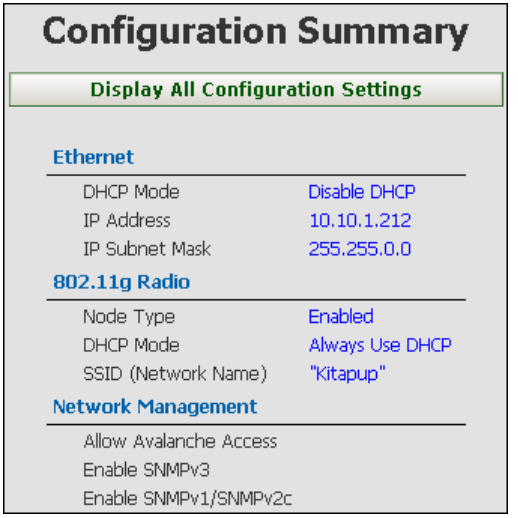
You can use the LEDs to help locate a specific IF5 in your location.

To locate an IF5

- In the About This IF5 RFID Reader screen, click **Find This IF5.** The middle three LEDs on the IF5 start flashing, while the two LEDs on the ends are unchanged. The LEDs flash until you click **Finished Finding IF5**.

Viewing the IF5 Configuration Summary

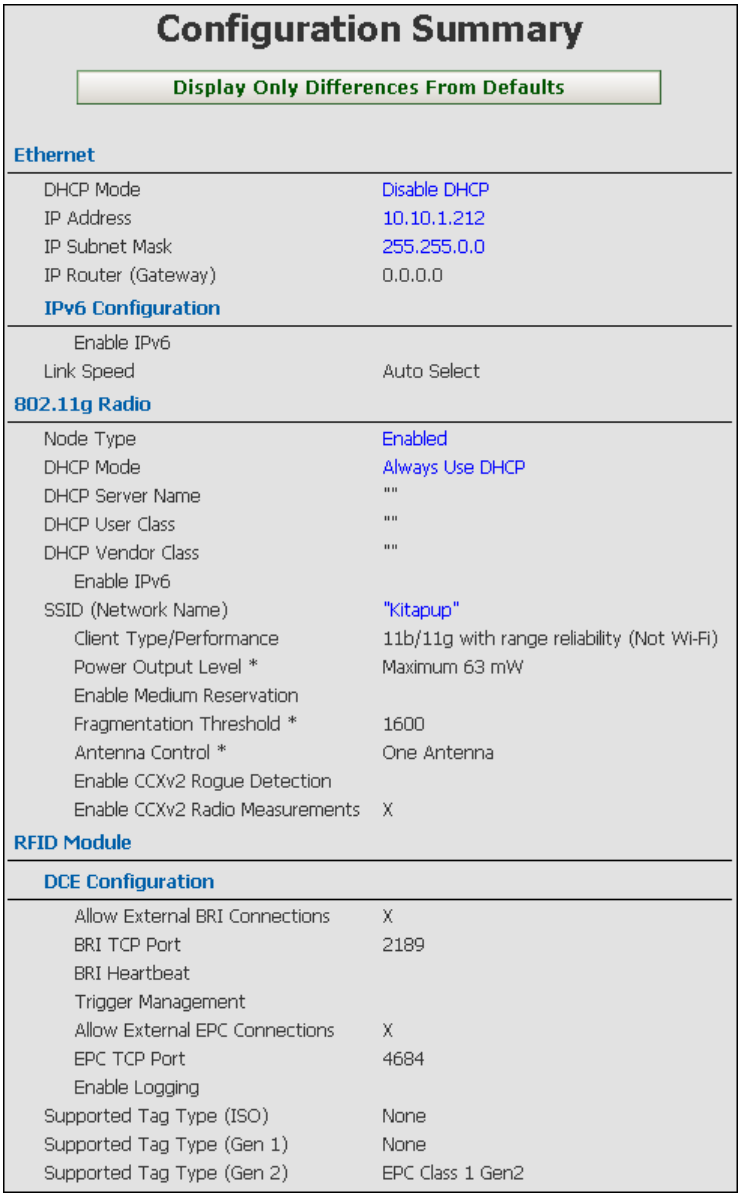
The About This IF5 RFID Reader screen includes a summary that shows basic parameter settings. Parameters that have been changed from the default configuration appear in blue.



Follow the next procedure to see a complete list of settings.

To view all IF5 configuration settings

- In the About This IF5 RFID Reader screen, click **Display All Configuration Settings**. The screen refreshes and shows a complete list of settings.



Configuration Summary

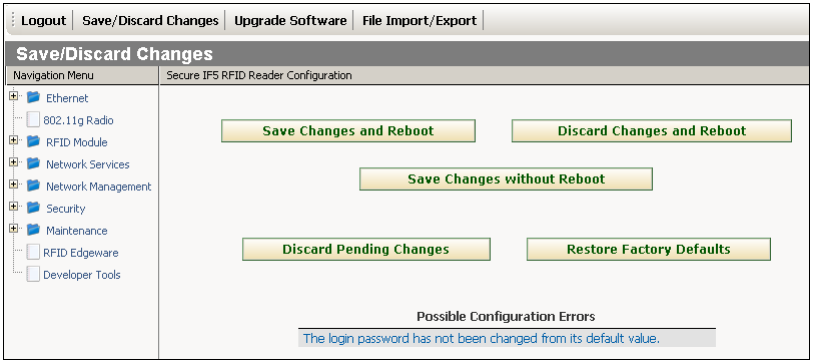
Display Only Differences From Defaults

Ethernet	
DHCP Mode	Disable DHCP
IP Address	10.10.1.212
IP Subnet Mask	255.255.0.0
IP Router (Gateway)	0.0.0.0
IPv6 Configuration	
Enable IPv6	
Link Speed	Auto Select
802.11g Radio	
Node Type	Enabled
DHCP Mode	Always Use DHCP
DHCP Server Name	""
DHCP User Class	""
DHCP Vendor Class	""
Enable IPv6	
SSID (Network Name)	"Kitapup"
Client Type/Performance	11b/11g with range reliability (Not Wi-Fi)
Power Output Level *	Maximum 63 mW
Enable Medium Reservation	
Fragmentation Threshold *	1600
Antenna Control *	One Antenna
Enable CCXv2 Rogue Detection	
Enable CCXv2 Radio Measurements	X
RFID Module	
DCE Configuration	
Allow External BRI Connections	X
BRI TCP Port	2189
BRI Heartbeat	
Trigger Management	
Allow External EPC Connections	X
EPC TCP Port	4684
Enable Logging	
Supported Tag Type (ISO)	None
Supported Tag Type (Gen 1)	None
Supported Tag Type (Gen 2)	EPC Class 1 Gen2

To hide parameter settings that have not been changed from the default values, click **Display Only Differences From Defaults**. The screen refreshes and shows only parameters changed from the default values.

Restoring the IF5 to the Default Configuration

1 From the menu, click **Save/Discard Changes**. The Save/Discard Changes screen appears.



2 Click **Restore Factory Defaults**. A list of the parameters that will be changed appears in the **Pending Changes** list.

3 Click **Save Changes and Reboot**. The IF5 reboots and the default configuration is restored.

Troubleshooting the IF5

This section includes lists of problems and possible solutions.

Problems While Working With RFID

Many problems you may encounter when working with your RFID system can be solved by carefully checking the RFID settings and changing them accordingly. For help, see "Configuring RFID Settings" on page 74.

RFID Problems and Solutions

Problem	Solution
The IF5 is unable to read RFID tags, or seems to read tags slowly or inconsistently.	Check these conditions: • Your RFID antennas must be connected correctly to the IF5 and mounted in optimum locations. Make sure all antenna connections are tight and that the cables are in good condition. For help, contact your Intermec RFID system consultant. • Terminators must be installed on all unused RFID antenna ports. If you have operated the IF5 without terminators on all unused antenna ports, the RFID module may be damaged. For help, contact Intermec Product Support. • To maximize IF5 performance, make sure you have chosen the correct Tag Type for your application. For help, see "Configuring RFID Settings" on page 74.
The IF5 does not respond to your RFID application.	Your application may not be connected to the IF5 Data Collection Engine (DCE). Check these conditions: • Make sure that you have disabled the IF5 Developer Tools or SAP Device Controller edgeware. For help, see "About IF5 Edgeware" on page 71. • You may need to change DCE settings to communicate with your application. For example, if your application is running on a desktop PC, you need to enable external BRI connections to the IF5. For help, see "Configuring the Data Collection Engine" on page 80.

RFID Problems and Solutions (continued)

Problem	Solution
The SAP device controller does not connect to the SAP backend module installed on your server.	Check these conditions: • Make sure you have enabled the SAP device controller edgeware on the IF5. For help, see "About IF5 Edgeware" on page 71. • Check the SAP device controller configuration files and make sure you have the correct information for your SAP system. For help, see "About the SAP-DC Configuration Files" on page 143.

Problems With Connectivity

When troubleshooting problems with connectivity, make sure you know and understand these network-specific items:

- TCP/IP settings
- Wireless network settings, including the SSID, 802.1x security, user names, and passwords
- COM port settings for serial connections

You should also make sure all physical network connectors and cables are in good working order.

Connectivity Problems and Solutions

Problem	Solution
You have assigned a static IP address to the IF5 but cannot connect to the IF5 over your network.	Make sure that DHCP is disabled and that your TCP/IP parameters are set correctly. For help, see "Configuring the IF5 (Setting the IP Address)" on page 10.
You cannot consistently maintain the 802.11g radio connection to the IF5.	You may need to move the IF5 so its 802.11g radio antenna is in a better position for the IF5 mounting location and your network. Make sure the antenna is connected to antenna port 4.
You cannot connect to the IF5 via Telnet.	Make sure that Telnet access is enabled on the IF5. For help, see "Controlling Developer Access" on page 44.
You cannot access the IF5 FTP directory.	Make sure that the IF5 FTP server is enabled. For help, see "Controlling Developer Access" on page 44.

Connectivity Problems and Solutions (continued)

Problem	Solution
You cannot connect to the IF5 through its 802.11g radio.	Make sure the radio is enabled and that your 802.11g radio parameters are set correctly, including all necessary security parameters such as user name and password. To check these settings when the radio does not work, you can either: • connect to the IF5 via HyperTerminal. For help, see "Using a Communications Program" on page 10. • connect to the IF5 through a wired Ethernet connection. For help, see "Using the Web Browser Interface" on page 19.
You cannot load a security certificate.	You must use a secure web browser connection to load certificates. For help, see "Using the Web Browser Interface" on page 19.
You cannot mount an NFS drive.	Make sure that NFS mounting is enabled on the IF5. For help, see "Controlling Developer Access" on page 44.
You cannot connect to the IF5 using the serial port.	**1** Verify that you are not using a crossover cable if connected to a hub or switch. Verify that you are using a crossover cable if connected directly to the PC or server. **2** Verify that you are communicating through the correct serial port. **3** Verify that your PC is set to 9600, N, 8, 1, no flow control.
You cannot connect to the IF5 using a web browser.	**1** Verify that you are not using a crossover cable if connected to a hub or switch. Verify that you are using a crossover cable if connected directly to the server or PC. **2** Open a HyperTerminal session to the IF5, and verify that you did not disable browser access in the Security screen. **3** If you access the Internet through a proxy server, be sure you have added the IP address of the IF5 to the Exceptions list. **4** Depending on the security configuration of your network, the IF5 may need to be on the same subnet as the nearest access point.

Problems With Copying Files

When copying files, there are two main problems that may occur:

- If the IF5 seems to be locked up when you try to copy files, the directory on the IF5 may be full. To check the available disk space, open a Telnet connection to the IF5. At the $-prompt, type `df` and press **Enter**. A report on the available disk space appears. Delete files if necessary and try copying the files again.

  For help with Telnet, see "Opening a Telnet Session to the IF5" on page 141.

- To copy files using the IF5 FTP server or an NFS server, you need to enable those access methods before copying files. For help, see "Controlling Developer Access" on page 44.

Calling Intermec Product Support

You may need to call Intermec Product Support if you have problems operating the IF5. Before calling, be sure you can answer the following questions:

- What kind of network are you using?
- What were you doing when the error occurred?
- What error message did you see?
- Can you reproduce the problem?
- What versions of IF5 and RFID software are you using? For help, see "Viewing the About This IF5 RFID Reader Screen" on page 114.

When you have these answers, call Intermec Product Support at 1-800-755-5505.

Upgrading Firmware

This section explains how to import and install IF5 and RFID firmware upgrades to the IF5.

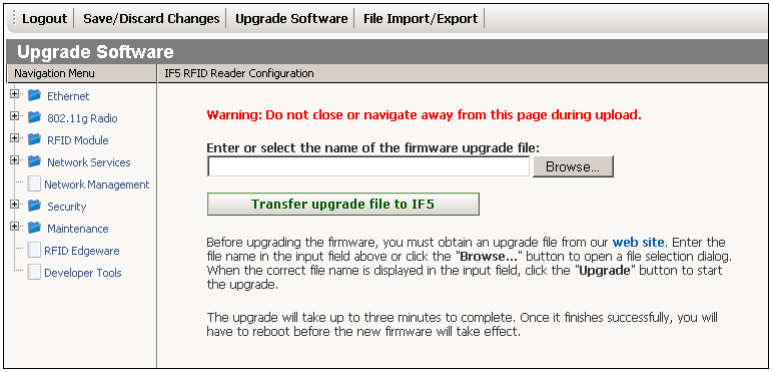
Note: To upgrade the firmware, use only files provided by Intermec. Be sure to contact your Intermec RFID system consultant before upgrading.

Caution

Make sure the IF5 is connected to a reliable AC power source before you upgrade the firmware. Do not cycle power to the IF5 during the upgrade. If AC power is lost during the upgrade, the IF5 may require factory repair.

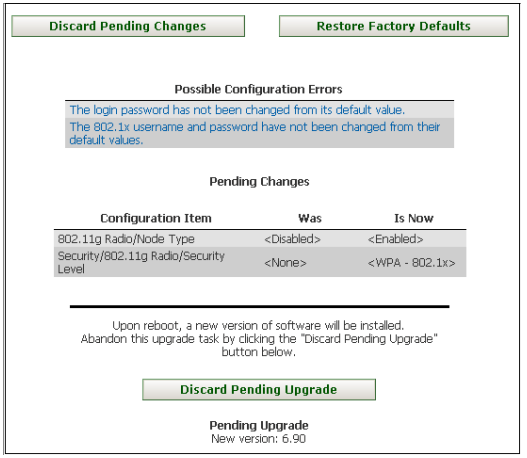
To upgrade the firmware

1 From the menu, click **Upgrade Software**. The Upgrade Software screen appears.


Logout
Save/Discard Changes
Upgrade Software
File Import/Export
Upgrade Software
Navigation Menu
IF5 RFID Reader Configuration
Ethernet
802.11g Radio
RFID Module
Network Services
Network Management
Security
Maintenance
RFID Edgeware
Developer Tools
Warning: Do not close or navigate away from this page during upload.
Enter or select the name of the firmware upgrade file:
Browse...
Transfer upgrade file to IF5
Before upgrading the firmware, you must obtain an upgrade file from our web site. Enter the file name in the input field above or click the "Browse..." button to open a file selection dialog. When the correct file name is displayed in the input field, click the "Upgrade" button to start the upgrade.
The upgrade will take up to three minutes to complete. Once it finishes successfully, you will have to reboot before the new firmware will take effect.

2 Click **Browse** to browse to the location of the upgrade file, and then double-click the filename. The name of the file appears in the **Enter or select the name of the firmware upgrade file:** entry field.

3 Click **Transfer upgrade file to IF5**. The file is transferred to the IF5. When this process is done, the Save/Discard Changes screen appears. The new firmware version appears under Pending Upgrade. You may need to scroll to see this part of the screen.


Discard Pending Changes
Restore Factory Defaults
Possible Configuration Errors
The login password has not been changed from its default value.
The 802.1x username and password have not been changed from their default values.
Pending Changes
Configuration Item
Was
Is Now
802.11g Radio/Node Type
<Disabled>
<Enabled>
Security/802.11g Radio/Security Level
<None>
<WPA - 802.1x>
Upon reboot, a new version of software will be installed.
Abandon this upgrade task by clicking the "Discard Pending Upgrade" button below.
Discard Pending Upgrade
Pending Upgrade
New version: 6.90

4 To continue the upgrade, click **Save Changes and Reboot**. The Rebooting screen appears, the IF5 reboots, and the upgrade begins. This process can take several minutes. Do not cycle power to the IF5 during the upgrade. When the upgrade process is complete, the IF5 reboots.

Or, to cancel the upgrade, click **Discard Pending Changes**.

5 Using the IF5 GPIO Interfaces

This chapter explains how to access the IF5 general purpose input/output (GPIO) interfaces and how to connect industrial controls such as motion sensors or indicator lamps to the IF5.

About the GPIO Interfaces

The IF5 has four general purpose input and output (GPIO) interfaces. You connect external controls such as motion sensors or indicator lamps to the GPIO interfaces, which can then trigger IF5 operations.

Each interface is electrically isolated from the IF5 and designed for low voltage DC loads. The IF5 can also supply 12VDC at 0.5A to external devices.

How the inputs and outputs are used depends on the RFID application software being used in the system. You need to coordinate input and output control wiring with the software developer.

Accessing the Interfaces

You can access the GPIO interfaces through the control port on the front panel of the IF5. The control port uses a standard 25-pin serial cable. For port pin assignments, see "Port Pin Assignments" on page 137.

You can also use the GPIO Terminal Block accessory to connect devices to the IF5 GPIO interfaces. The block provides access to the IF5 GPIO interfaces via standard screw terminals.

GPIO Terminal Block accessory

For more information on the terminal block, contact your local Intermec distributor.

Using the Input Interfaces

Each of the four inputs is compatible with input signals of 10 to 48 VDC. Both the high and low signal contacts are exposed and isolated to 1500V. Input impedance is 1.8K minimum.

GPIO Input Signal Descriptions

Signal	Description	Min.	Typical	Max.
V_{in} (High)	High input voltage	10V	24V	48V
V_{in} (Low)	Low input voltage	-1V	0V	1V

In a typical application, the IF5 senses input from an external control like a switch and then starts a tag read operation.

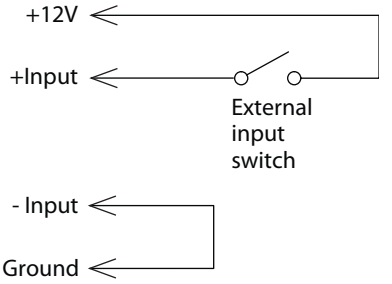
There are three basic ways to connect input controls to the IF5 input interfaces:

- Supply the input interface with power from the IF5.
- Isolate the IF5 from the input power source.
- Use an open collector solid state drive from a remote device to control the inputs.

For more information, see the next examples.

IF5 Powered Input

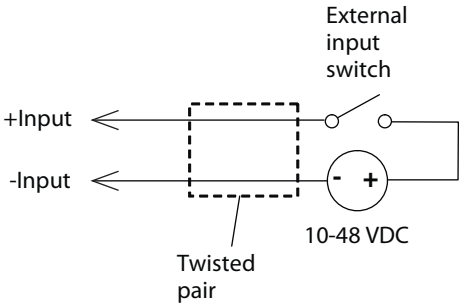
This is the simplest way to connect a control to an IF5 input interface. If the external control device is a switch, you can connect one side of the switch to an IF5 +Input pin, and the other side of the switch to one of the +12 VDC sources. Ground the corresponding -Input pin as shown in the next illustration.



IF5 Powered Input

Isolated Input Interface

Use this method to minimize noise induced by distance or grounding characteristics. The isolated input avoids induced noise by referencing a remote input to chassis return of the IF5. The next illustration shows how this method is wired.

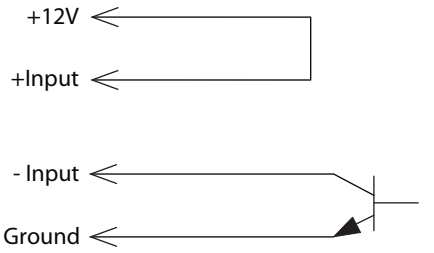


Isolated Input Interface

Open Collector Input Interface

The input can be connected to an open collector interface of an external device. This typically implies that the grounds are tied together for the two systems. The common ground can be a source of input noise, so you should follow good grounding practices for both the IF5 and the input device.

In this situation, the IF5 provides power to the pull-up resistor for the open collector. Connect the +Input pin to the +12 VDC source as shown in the next illustration.



Open Collector Input Interface

Using the Output Interfaces

Each IF5 output interface is optically isolated from the IF5, polarized, and rated for 5 to 48 VDC at 0.25A. All IF5 outputs include internal thermal fuses that trip if the load exceeds 0.25A, and the fuses are self-recovering once the excessive load is removed. The high and low contacts are exposed and isolated from ground. Transient suppression limits output voltage spikes to 65 VDC.

GPIO Output Specifications

Signal	Description	Min.	Typical	Max.
Leakage current (High)	Switch output, high leakage current	0 mA	1 mA	10 mA
V_{sat} (Low)	Switch output on, saturation voltage with .25A load	0V	1V	1.5V

Because the outputs are optically isolated, each one can be configured to switch the high side or the low side of the load. You can power the load directly from the IF5 or from an external power supply.

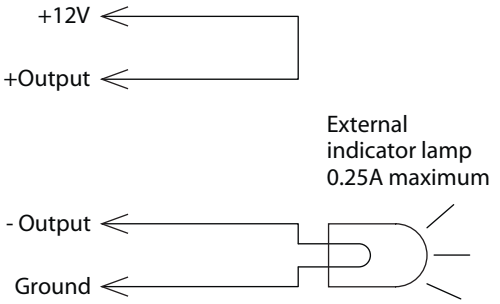
In a typical application, the outputs control indicator lamps that signal good reads or errors. The basic methods for connecting external devices to the GPIO outputs include:

- Switching the high side, with the load powered by the IF5
- Switching the low side, with the load powered by the IF5
- Switching the high side, with the load powered externally
- Driving a DC relay that controls an AC load

These methods are shown in the next examples.

Switching the High Side Using IF5 Power

In this example, an external indicator lamp (0.25A maximum current) is connected to the -Output and Ground pins, and the corresponding +Output pin is connected to the +12 VDC source.

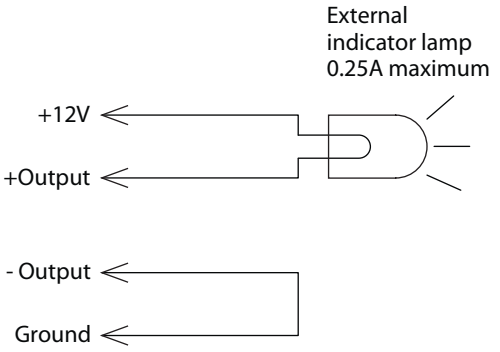


Switching the High Side

Switching the Low Side Using IF5 Power

For low side switching applications, the lamp power is routed to all the lamps in common and the low side of the load is routed to the switch.

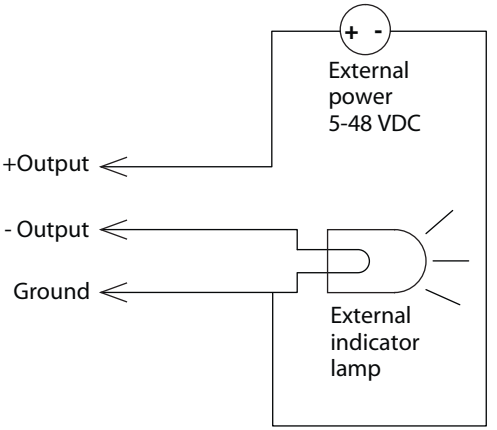
In this method, connect the external indicator lamp to the +Output and +12 VDC pins, and short the corresponding -Output pin to ground as shown.



Switching the Low Side of the Output Load

Switching the High Side Using External Power

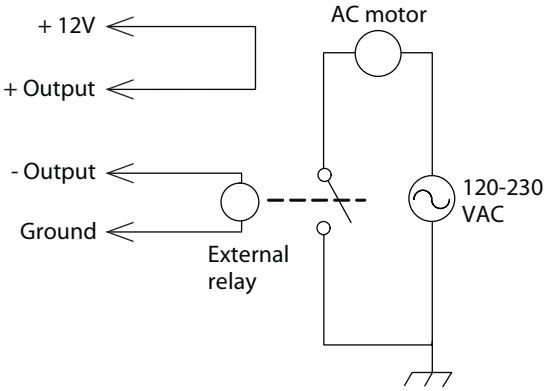
To use external power (5 to 48 VDC) to switch the high side, connect the Ground pin to the ground system of the external power supply, and connect the positive side of the external supply to the +Output pin. The external indicator lamp is connected to the corresponding -Output and Ground pins as shown in the next illustration.



Switching the High Side With External Power

Driving a DC Relay to Control an AC Load

While the IF5 outputs are designed to switch DC loads, they can drive relays that control AC loads. The next illustration shows how to connect such a system to an IF5 output.



Driving a DC Relay: *The external relay provides dry contacts for controlling the AC motor.*

Note: In many installations, the relay and AC wiring must be placed in an enclosure that meets local fire code regulations.

Using the Power Interface

The IF5 GPIO interface provides 12 VDC at 0.5A for powering external inputs and loads, eliminating the need for an external DC supply and simplifying the system installation.

The GPIO interface power has an internal thermal fuse that trips if the load exceeds 0.5A. The fuse is self-recovering once the excessive load is removed.

The total load on the GPIO interface power must stay within the 0.5A limit. When you design a system that uses the GPIO interface power, be sure to complete a power budget assessment to ensure that the supply is adequate for the system.

If your system needs more than +12 VDC at 0.5A, you can connect an external power supply to the +12V and Ground pins. The external supply powers the external loads, and that power will be available at all +12V pins on the control port.

A Specifications

This appendix includes physical and electrical specifications for the IF5 and information about the port pin assignments.

IF5 Specifications

Height	9.5 cm (3.8 in)
Length	35.5 cm (14.0 in)
Width	23.6 cm (9.3 in)
Weight	2.63 kg (5.8 lb)
AC electrical rating	~ 100 to 240V, 1.0 to 0.5A, 50 to 60 Hz
Operating temperature	-25ºC to +55ºC (-13ºF to +131ºF)
Storage temperature	-40ºC to +70ºC (-22ºF to +158ºF)
Humidity (non-condensing)	10 to 90%
Ethernet interfaces	10BaseT/100BaseTx (twisted-pair)
Ethernet compatibility	Ethernet frame types and Ethernet addressing
Ethernet data rate	10 Mbps/100 Mbps
Radios supported	802.11g
Serial port maximum data rate	115,200 bps
SNMP agent	RFC 1213 (MIB-2), RFC 1398 (dot3), 802.11, 802.1x
Linux version	2.6.11.5

802.11g Radio Specifications

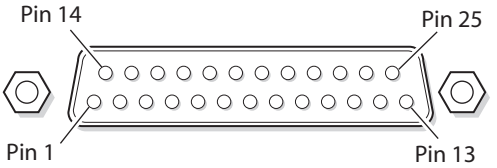
Frequency band	2.4 to 2.5 GHz worldwide
Type/Modulation	Direct sequence, spread spectrum (CCK, DQPSK, DBPSK)
Power output	63 mW (18 dBm)
Basic data rate	11, 5,5, 2, and 1 Mbps
Extended data rate	54, 48, 36, 24, 18, 12, 9, and 6 Mbps
Channels	11 (North America), 13 (Europe, Japan), 4 (France), 1 (Israel)
Range (Maximum power output, 11 Mbps)	160 m (525 ft) open environment 50 m (165 ft) semi-open environment 24 m (80 ft) closed environment Unlimited range with roaming. Lowering power output reduces range.
Receiver sensitivity (11 Mbps)	-82 dBm
Security	WEP, Dynamic WEP 802.1x, WPA-PSK, WPA2-PSK, WPA-802.1x, WPA2-802.1x

RFID Specifications

Protocols Supported	EPCglobal Class 1 Gen 2 ISO 18000-6B Generation 1 ISO 18000-6B Generation 2 Phillips v1.19
Frequency Range	865-868 MHz, 869 MHz, or 915 MHz
Usable channels	1
Output power	
865-867 MHz, 915 MHz	Minimum: 28.5 dBm Typical: 29.5 dBm Maximum: 30.0 dBm
869 MHz	Minimum: 25.5 dBm Typical: 26.5 dBm Maximum: 27.0 dBm
Occupied frequency bandwidth	<250 KHz
Tag data rate	32 kbps/160 kbps
Dispatch rates	
Tag ID rate	70 tags per second
Tag data exchange rate	Reads a tag containing 8 bytes of data within 12 ms. Performs a verified write to a tag at an average rate of 31 mS per byte per tag.
Write range	Up to 70% of the read distance under similar conditions
Transmitter type	90% amplitude modulation index
Frequency stability	<±100 ppm from -25°C to +55°C (-13°F to 131°F)
Number of antennas	Up to 4, electronically switched
Antenna port isolation	22 dB
Antenna connectors	865-867 MHz: SMA 915 MHz: Reverse SMA

Port Pin Assignments

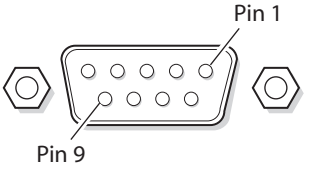
Control Port



Control Port Pin Assignments

Pin	Description	Active Polarity
1	-Input 1	Low-RTN
2	-Input 2	Low-RTN
3	-Input 3	Low-RTN
4	-Input 4	Low-RTN
5	Ground	
6	Ground	
7	+Output 1	High (10-48V)
8	Ground	
9	+Output 2	High (10-48V)
10	Ground	
11	+Output 3	High (10-48V)
12	Ground	
13	+Output 4	High (10-48V)
14	+Input 1	High (10-48V)
15	+Input 2	High (10-48V)
16	+Input 3	High (10-48V)
17	+Input 4	High (10-48V)
18	12VDC	
19	-Output 1	Low-RTN
20	12VDC	
21	-Output 2	Low-RTN
22	12VDC	
23	-Output 3	Low-RTN
24	12VDC	
25	-Output 4	Low-RTN

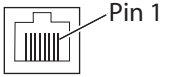
Serial Port



Serial Port Pin Assignments

Pin	Description	Active Polarity
1	NC	
2	Receive data (RXD)	High
3	Transmit data (TXD)	High
4	NC	
5	Signal ground	
6	NC	
7	NC	
8	NC	
9	NC	

Ethernet Port



Ethernet Port Pin Assignments

Pin	Description	Pin	Description
1	LAN_RX+	5	VDC_A
2	LAN_RX-	6	LAN_TX-
3	LAN_TX+	7	VDC_B
4	VDC_A	8	VDC_B

Note: The IF5 does not support power over Ethernet (POE).

B Configuring and Using the SAP Device Controller

This appendix explains how to use the SAP device controller edgeware on the IF5. It includes a section that explains how to use the SAP data processors with tag data.

Enabling the SAP Device Controller

This section explains how to enable and use the SAP device controller on the IF5. In your SAP system, the controller communicates with an SAP Auto-ID Infrastructure (SAP-AII) server. On the IF5, the device controller software is installed in the /usr/local/dc directory.

Note: Before you can use the SAP device controller, you need to disable other RFID edgeware and enable the device controller. When the controller is enabled, it automatically starts whenever the IF5 is booted. For help, see "About IF5 Edgeware" on page 71.

To configure and enable the SAP device controller

1. Start the web browser interface. For help, see "Using the Web Browser Interface" on page 19.
2. Assign a static IP address to the IF5. For help, see "Configuring the IF5 (Setting the IP Address)" on page 10.
3. (Optional) If actual time should be used in messages reported by the SAP device controller, set SNTP parameters. For help, see "Configuring SNTP Client Settings" on page 36.
4. Change settings in the SAP-DC configuration files as needed. For help, see "About the SAP-DC Configuration Files" on page 143.
5. Save your changes and reboot the IF5. For help, see "Saving Configuration Changes" on page 22.

Running the Device Controller Manually

When you enable the SAP device controller, it automatically starts when the IF5 is booted. You can also start, stop, and reconfigure the device controller manually via a Telnet session. For help, see the next section.

Note: To open a Telnet session, you need to enable Telnet shell access to the IF5. For help, see "Controlling Developer Access" on page 44.

Opening a Telnet Session to the IF5

1. On your desktop PC, start Telnet.
2. In the Telnet window, type `open xxx.xxx.xxx.xxx`, where *xxx.xxx.xxx.xxx* is the IP address of the IF5.
3. Press **Enter**. The login prompt appears.
4. Type `intermec` and press **Enter**. The password prompt appears.
5. Type `intermec` and press **Enter**. The $-prompt appears. Your Telnet session with the IF5 is established.

Starting and Stopping the Device Controller Manually

To start the device controller manually, open a Telnet session to the IF5 and send this command at the $-prompt:

```
/usr/local/dc/sapdc &
```

To stop the device controller manually, open a Telnet session to the IF5 and send this command at the $-prompt:

```
/usr/local/dc/dccontrol SHUTDOWN <port>
```

where *port* is the configured listening port. This parameter is required only if the device controller is not using the default listening port (9000).

Reconfiguring the Device Controller Manually

To reconfigure the device controller, first make your changes to the SDCConfiguration.xml file, and then open a Telnet session to the IF5. Send this command at the $-prompt:

```
/usr/local/dc/dccontrol RECONFIGURE
<MyDirectory><port>
```

where:

MyDirectory	is the URL of the new SDCConfiguration.xml file.
port	is the configured listening port. This parameter is required only if the device controller is not using the default listening port (9000).

Stopping or Reconfiguring the Device Controller Over the Network

When the device controller is running, you can stop or reconfigure the controller by sending an XML command message over HTTP to the configured listening port (typically port 9000).

To stop the device controller, send this command message:

```
<?xml version="1.0" encoding="utf-8"?>
<Command id="123456789" response="rec1">
   <Shutdown/>
</Command>
```

To reconfigure the device controller, send this command message:

```
<?xml version="1.0" encoding="utf-8"?>
<Command id="123456789" response="rec1">
   <Reconfigure URL="http://hostname/config.xml">
</Command>
```

where:

hostname	is the directory where the configuration file is located.
config.xml	is the name of the configuration file.

Using the Configuration File Generator

The device controller includes a generation script that creates default configuration files based on command line parameters. Using this utility you can quickly configure the device controller to connect to an SAP-AII node. The resulting configuration files are intended as a basis for further customization.

The script is located at /usr/local/dc/configsapdc and its syntax is as follows:

```
configsapdc <Aii-node-URL><port>
<device controller name><device name><DCE port>
```

where:

Aii-node-URL	is the URL of the SAP-AII node.
port	is the TCP port on which the device controller accepts SAP communications.
device controller name	is the name of this device controller in SAP-AII.
device name	is the name of this device in SAP-AII.
DCE port	is the TCP port supported by the DCE for BRI communications. Default is 2189.

The following example configures the device controller to connect to an SAP-AII server at “myhost” on port 50000 while accepting connections from SAP-AII on port 9000:

```
./configsapdc http://myhost:50000/sap/scm/ain 9000
IF5_DC IF5_001 2189
```

About the SAP-DC Configuration Files

The SAP device controller uses several configuration files:

- Config/SDCConfiguration.xml

  Main configuration file for the device controller. Not required if the SimpleDevice.property file points to other than this default location. For more information, see the next section.

- RfidReader.properties

  Defines hardware-specific settings, such as tag ID length or the number of Read tries. For more information, see “About the RfidReader.properties File” on page 148.

- Config/SimpleDevice.property

  Defines logging properties and the URL of the main configuration file for the device controller. This file is loaded at startup of the device controller. To use another filename, add the filename as an additional parameter to the command line when starting the device controller.

  For more information on logging, see “Setting Parameters for Logging” on page 151.

- Config/FieldMap.xml

Defines field maps that the device controller may use. A field map maps logical field names to specific tag memory addresses.

All the configuration files are stored on the IF5 in the /home/developer/dc directory.

Changing Settings in the Configuration Files

To change settings in the configuration files, you can:

- import the files from the IF5 to your desktop PC, make changes, and export the modified files to the IF5.
- use an application on your desktop PC to create new configuration files, and export the modified files to the IF5.

For help with importing and exporting files, see "Using the Web Browser to Import and Export Files" on page 104.

If you have enabled FTP access on the IF5, you can import and export files via FTP. For help, see "Using the FTP Server to Import and Export Files" on page 108.

To restore the default SAP-DC configuration files on the IF5, delete the /home/developer/dc/config directory on the IF5. When you reboot the IF5, the directory and default files are created by a startup script on the IF5.

About the SDCConfiguration XML File

This file defines settings that determine how event data is transmitted to the SAP-AII server. These settings are described next.

Controller ID

The Controller element has an ID attribute that should contain the ID of this device controller in the SAP system. For example, UNLOAD_GATE_IF5 is the controller ID attribute in this XML fragment:

```
<Configuration xmlns:opt="c:\">
   <Controller id="UNLOAD_GATE_IF5" description="Receiving Gate -
    Intermec IF5 Fixed Reader">
      <ReceiverList>
```

ReceiverList

This element specifies a list of destinations that receive RFID tag events from the device controller. Each Receiver element defines one destination, which is generally an SAP-AII node, and contains an id attribute that identifies the receiver. Other parts of the SDCConfiguration file may refer to this attribute. A receiver element also includes option list elements and a MessageTransformer element, which are described in the next table.

Element	Description
opt:Name	Name of the receiver. This name will be displayed in logs.
opt:URL	URL that receives tag event data when transmitted by the controller. For SAP-AII nodes, this is usually `http://mySAPserver:50000/sap/scm/aim`
opt:Port	Port used by the controller to receive commands from this receiver. Default is 9000.
opt:Synchronization	Defines the processing mode for handling commands. Always set to “asynchronous”.
MessageTransformer	Stores the name of the software component that formats messages transmitted to this receiver. Leave this setting at the default.

In the sample XML below, the Receiver element defines the SAP-AII node and defines the receiver id as “rec1”.

```
<ReceiverList>
   <Receiver id=”rec1” protocol=”HTTP” description=”SAP AII NODE”
      <OptionList>
         <opt:Name>SDCReceiver</opt:Name>
         <opt:URL>http://136.179.176.37:8080/DummyServlet</opt:URL>
         <opt:Port>9000</opt:Port>
         <opt:Synchronization>asynchronous</opt:Synchronization>
      </OptionList>
      <MessageTransformer>
<APIImplementationClass>com.sap.device.controller.messaging.
XMLTransformer</APIImplementationClass>
      </MessageTransformer>
   </Receiver>
</ReceiverList>
```

Reader List

This element defines the IF5 that the controller manages. The Reader id attribute defines the name of the IF5 in the SAP system. The LogicalName value is the name assigned to the reader in the RfidReader.properties file.

In the sample XML below, the IF5 name in the SAP system is "Fixed_Reader_18":

```
<ReaderList retryInterval="10">
   <Reader id="Fixed_Reader_18" description="Reader">
      <LogicalName>IF5_reader1</LogicalName>
   </Reader>
</ReaderList>
```

FieldMap

This element defines the location of the field map definitions, and generally points to the FieldMap.xml file in the home/developer/cd/config directory on the IF5. The defaultTable attribute specifies which Table element in the .xml file will be used to map RFID tag fields. In the next example, the defaultTable is defined as "Intermec".

```
<FieldMap defaultTable="Intermec">file:config/FieldMap.xml</FieldMap>
```

ExtensionCommandHandler

This element defines the software component that processes VendorExtension commands from receivers. Do not change this element.

ProcessorChainList

This element defines the data processors of your system and how they are linked together. For more information, see "Using the Data Processors" on page 152.

The ProcessorChainList contains a DataProcessorList and a LinkList. The DataProcessorList element contains a list of data processors that the system contains. Each data processor is defined in a DataProcessor element as shown in this example:

```
        <DataProcessor id="agg" description="Aggregation">
          <APIImplementationClass>
com.sap.devicecontroller.core.dataprocessors.TimeFixedSizeAggregator
          </APIImplementationClass>
          <OptionList>
            <opt:TimerInterval>1000</opt:TimerInterval>
            <opt:MaxCount>1000</opt:MaxCount>
          </OptionList>
        </DataProcessor>
```

About the DataProcessor Element

A DataProcessor element has an id attribute used to refer to this data processor in other parts of the xml file. It also contains two subelements as described next:

Subelement	Description
APIImplementationClass	Specifies the Java class that implements the data processor. Data processor implementations are generally in the com.sap.devicecontroller.core.dataprocessors package. For a complete list of available data processors, see the SAP documentation.
OptionList	A list of configuration options that the data processor will use to determine its behavior. The available options and their effects are specific to each data processor implementation. By convention, each option element in the option list is named prefaced with “opt:”.

About the LinkList Element

The LinkList element defines how the data processors are connected together and includes two subelements as described next:

Subelement	Description
ToDP	Specifies the data processor events will come from. Use the DataProcessor element ‘id’ attribute to specify a data processor.
FromDP	Specifies the data processor events will go to. Use the DataProcessor element ‘id’ attribute to specify a data processor.

The device controller default configuration specifies a sample pipeline. Make sure that ReaderIDs specified in ProcessorChainList match the Reader ids of the reader definitions in ReaderList as shown in the next example.

```
<ReaderList retryInterval="10">
   <Reader id="Fixed_Reader_18" description="Reader">
      <LogicalName>IF5_reader1</LogicalName>
   </Reader>
</ReaderList>
      .
      .
      .
<ProcessChainList>
   <DataProcessorList>
      <DataProcessor id="lp" description="LowPassFilter">
<APIImplementationClass>com.sap.devicecontroller.core.dataprocessors
.LowPassFilter</APIImplementationClass>
        <OptionList>
          <opt:ReaderID>Fixed_Reader_18</opt:ReaderID>
          <opt:TimerInterval>500</opt:TimerInterval>
        </OptionList>
     </DataProcessor>
```

About the RfidReader.properties File

This .xml file defines properties specific to the IF5 RFID module. RfidReader.properties.xml must reside in the /home/developer/dc directory on the IF5.

The next table lists properties you can set for BRI implementation. For more information on reader-specific properties, see the *Basic Reader Interface Programmer's Reference Manual* (P/N 937-000-xxx).

Element	Default	Description
Name	-	(Required) Defines the name of this reader. Used in the main XML configuration file as "LogicalName" to reference this reader.
Classname	-	(Required) Sets the LLI Java implementation class for this reader. Always use com.sap.readerImplementations.intermec.IntermecBRIReader.
readerAddress	-	(Required) Specifies the IP address of the reader. If the SAP device controller is running on the reader directly, set to localhost or 127.0.0.1.
readerPort	-	(Required) Specifies the TCP/IP port to use for the BRI interface. Set to 2189.

Element	Default	Description
pollingInterval	0	(Optional) Sets the interval in ms between READ commands sent by the reader. The polling loop can run continuously, or can be started by a trigger and run for a period set by trigger.time.
tagID.type	EPC	Defines the type of tag to be read: **EPC**: EPC tag ID stored on the tag in the standard location for that tag type. **ISO**: For UCODE 1.19 tags, this is the ISO tag ID, stored in the standard ISO tag ID location. For EPC Class 1 Gen 2 tags, the TID field is returned as the tag ID. **CUSTOM**: ID is stored in a customer-defined area in user memory on the tag. The tagID.address and tagID.length properties determine where the ID is stored on the the tag.
tagID.address	0	(Optional) Defines the memory address where the tag ID is stored. This can be used when some ID other than the manufacturer-set tag ID is desired. Set tagID.type to CUSTOM to define tagID.address. Use an integer to specify the memory address for ISO tag types. For EPC Class 1 Gen 2 tags, specify the address as <memory bank>:<memory address>. For example, specify “3:15” to choose memory bank 3 at address 15.
tagID.length	8	(Optional) Sets the length of the tag ID. Set tagID.type to CUSTOM to define tagID.length.
logFile	-	(Optional) Specifies the file name that BRI logs should be written to. If not set, no BRI logging occurs.
output.use	0	(Optional) Set to 1 to use GPIO output ports to indicate the operation the reader is performing.
output.mode.inactive	0	(Optional) When output.use=1, the outputs are set to this value when the reader is inactive.
output.mode. readingNoTags	0	(Optional) When output.use=1, the output ports are set to this value when the reader is reading and no tags are found in the field.

Element	Default	Description
output.mode.reading	0	(Optional) When output.use=1, the output ports are set to this value when the reader is reading and tags are found.
output.mode.writing	0	(Optional) When output.use=1, the output ports are set to this value when the reader is writing to a tag.
trigger.mode	NONE	(Optional) Sets GPIO state that fires a trigger operation: **NONE**: No triggers are used. **AND**: A single trigger is used. To fire, the value on the GPIO ports bitwise ANDed with trigger.mask must equal trigger.value. **OR**: Not supported by this release.
trigger.value	1	(Optional) Sets the value that must be on the GPIO ports to fire a trigger.
trigger.mask	15	(Optional) Sets the mask used for the GPIO ports value.
trigger.time	1000	(Optional) Sets the time in ms during which the reader tries to find tags after a trigger is fired. Also sets the time that passes before the trigger fires again.
idTries	2	(Optional) Sets the ID tries.
readTries	3	(Optional) Sets the Read tries.
writeTries	3	(Optional) Sets the Write tries.
selectTries	1	(Optional) Sets the Select tries.
unselectTries	1	(Optional) Sets the Unselect tries.
lockTries	254	(Optional) Sets the Lock tries.
initTries	1	(Optional) Sets the Initialization tries.
antennaTries	3	(Optional) Sets the Antenna tries.
antennas	1,2,3,4	(Optional) Sets the antennas to be used and the firing sequence for those antennas.
tagType	UCODE119	(Optional) Defines the type of tags to be read: **G1**: ISO Class 1 Gen 1 tags **G2**: ISO Class 1 Gen 2 tags **UCODE119**: Phillips v1.19 tags **EPCC1G2**: EPC Class 1 Gen 2 tags **MIXED**: Mixed groups of tags

Element	Default	Description
GPIOValue.green	-	(Optional) Sets the value of the GPIO output lines in response to a GREEN ExtensionCommand.
GPIOValue.yellow	-	(Optional) Sets the value of the GPIO output lines in response to a YELLOW ExtensionCommand.
GPIOValue.red	-	(Optional) Sets the value of the GPIO output lines in response to a REDExtensionCommand.

Note: To handle custom ExtensionCommand strings, more GPIOValue.xxx properties can be added. The command string name must be in lowercase characters in the .xml file.

For example, to make the controller respond to a BUZZER ExtensionCommand by setting GPIO output lines to 7, add this property: `GPIOValue.buzzer=7`

Setting Parameters for Logging

The SimpleDevice.property file sets parameters for logging. The SAP device controller uses the SAP logging API. There are two types of logs:

- Traces (LOCATION), for developers to use when debugging
- Logs (CATEGORY), for administrators monitoring regular operation

You can define a log level and format for each type. Logging can be done to the console, a file, or both. You can also log to a rotating set of files instead of a single file.

For the IF5 SAP device controller, Intermec recommends using the /tmp directory (or a subdirectory thereof) for best performance.

The next example shows a sample SimpleDevice.property file.

```
URL=file:config/SDCConfiguration.xml
LOCATION_LEVEL=ALL
LOC_TYPE=BOTH
LOC_FILENAME=/tmp/dc%g.trc
LOC_MAXFILESIZE=32000
LOC_NO_OF_FILES=10
LOC_FORMATTER=TRACE
CATEGORY_LEVEL=NONE
CAT_TYPE=FILE
```

```
CAT_FILENAME=/tmp/dc%g.log
CAT_MAXFILESIZE=32000
CAT_NO_OF_FILES=10
CAT_FORMATTER=TRACE
```

Logging parameters are described in the next table.

Parameter	Description
LOCATION_LEVEL, CATEGORY _LEVEL	Sets the type of values to be logged: ALL, DEBUG, PATH, INFO, WARNNING, ERROR, FATAL, NONE
LOC_TYPE, CAT_TYPE	Sets the location of the logging: FILE, CONSOLE, or BOTH
LOC_FILENAME, CAT_FILENAME	Sets the name of the log file. Required if LOC_TYPE is set to FILE or BOTH. Use the format <filename>.
LOC_MAXFILESIZE, CAT_MAXFILESIZE	Sets the maximum size of the logfile. Use the format <integer>. Default is FileLog.NO_LIMIT. Required only if LOC_TYPE is set to FILE or BOTH.
LOC_NO_OF_FILES, CAT_NO_OF_FILES	Sets the number of logfiles if you want to log to more than one file. Use the format <integer>. Default is FileLog.NO_CNT. Required only if LOC_TYPE is set to FILE or BOTH.
LOC_FORMATTER, CAT_FORMATTER	Sets the format for the logfile entries: XML, LIST, or TRACE. XML and TRACE supported only if you are running the controller with the J2SE engine.

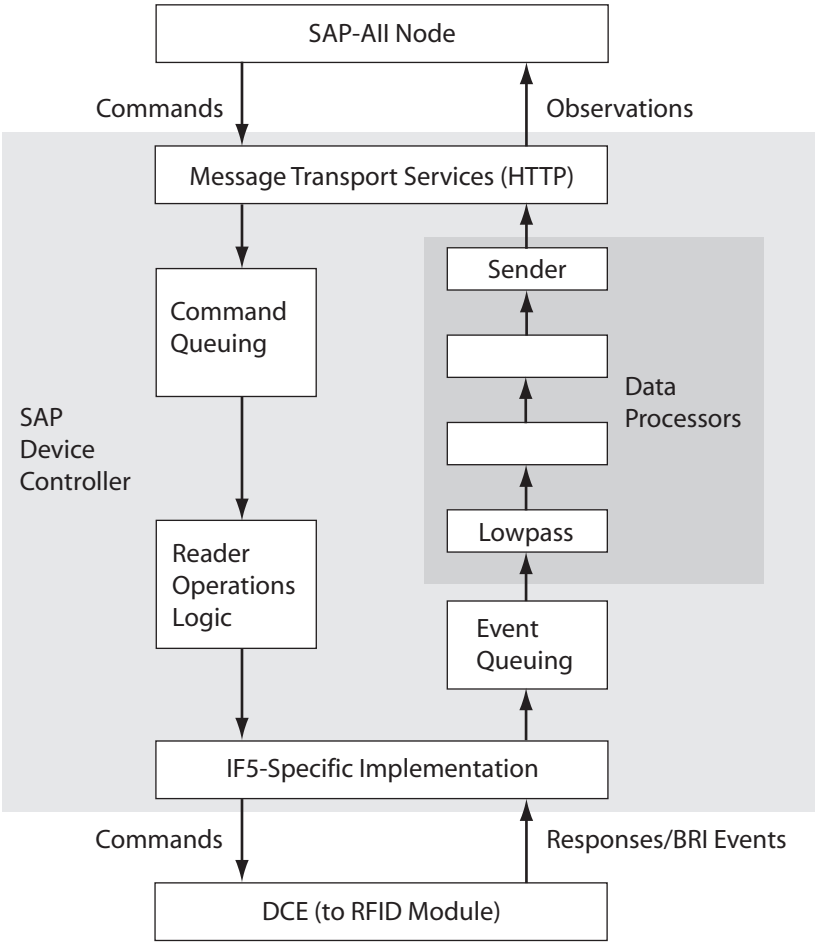
Using the Data Processors

SAP defines a data processor as a simple component implementing a special function. Data processors are used to:

- process events from RFID readers asynchronously.
- send the processed events to SAP-AII.

Data processors can be arranged flexibly and added as necessary to add sophisticated event filtering to your system.

The next diagram shows the relationship of data processors to other aspects of the system with regard to command and data flow:



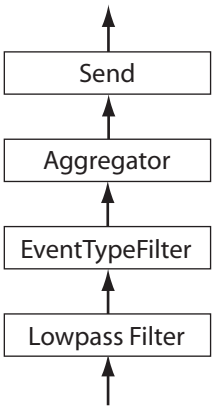
Data Processor Flow Chart: *This diagram shows how data processors are integrated into SAP command and data flow.*

Data Processor Types

There are five main types of data processors:

- **Enrichers** read additional data from the tags (or other sources) and add this data to the data structure of the event.
- **Writers** write data to or change data on the tags.
- **Filters** filter out certain events according to some criteria (for example, they could filter out all events coming from case tags, or clean out false "tagDisappeared" events ("low pass filter").
- **Buffers** buffer the events for later processing and keep an inventory of tags currently in the field.
- **Aggregators** aggregate several events into a single event so they can be transmitted in a single message, thereby improving system efficiency.
- **Senders** transform the internal data structure with the help of a Transformer and sends the information to registered recipients (generally SAP-AII).

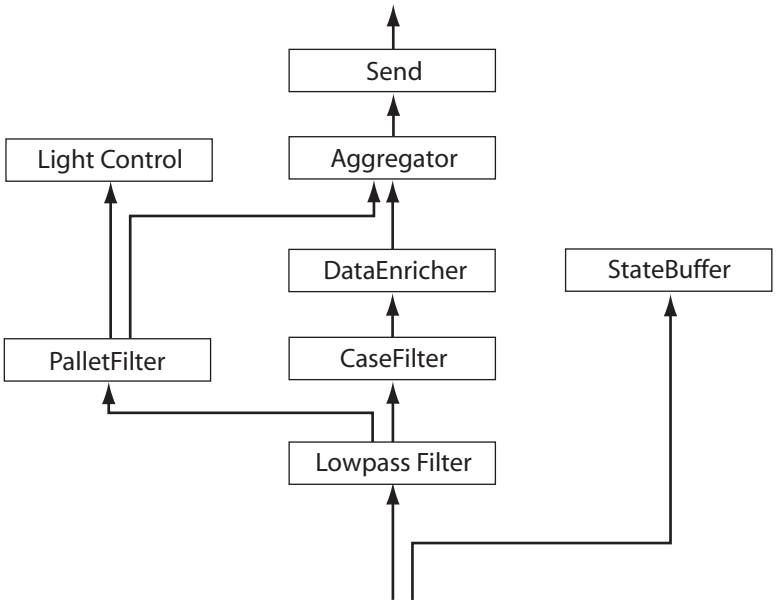
To achieve the desired functionality (filtering, aggregation, etc.), data processors are arranged into chains or meshes. A processor receives events, performs its function, and passes the events on to the next processor. The next illustration shows a simple data processor chain as specified in the default configuration:



Default data processor chain

This chain passes events through a low pass filter (to remove false "disappeared" events), filters out unwanted events using the EventType filter, bundles events together using the aggregator, and finally transmits the bundled events to SAP-AII using a Send data processor.

Data processor chains need not be linear. The theoretical example below processes tag events from pallets and cases differently. Pallets can set lights on a light tower while events from cases are augmented with user data from the tags (using a data enricher). This example assumes you have a tag data scheme set up so you can differentiate palettes and cases using the tag data.



Nonlinear data processing

Standard Data Processors

All data processors are implemented as Java classes in the com.sap.devicecontroller.core.dataprocessors package. The data processors that ship with SAP-DC are:

CheckReader

This processor checks if a reader is still working.

- It periodically checks all specified readers if they function properly by calling `identify()`. If the call does not throw an exception, the reader is considered as working. Otherwise the reader is disconnected and added to the ReaderErrorManager singleton.
- Received RfidEvents and DataProcessorEvents are forwarded to the next data processors in the chain. However, events where the tag ID equals the check tag ID are filtered out.

All tag IDs returned from `identify()` (except the check tag ID) are packaged in a DataProcessorEvent and forwarded.

DuplicateFilter

This class filters all events that appear or disappear twice (or more times) in a row. If the event is of type "APPEARED" or "DISAPPEARED", and received twice, the second event is ignored. For example, DuplicateFilter can be used when the Device Controller is monitoring a gate consisting of two or more physical readers that form one logical read point.

SimpleDuplicateFilter

Filters out all duplicate tags of the same type (appeared/disappeared), regardless of which reader the tags came from. This simple duplicate filter does not maintain a history of past events and only filters duplicates in the current event message it is processing. Use SimpleDuplicateFilter inside a chain after an aggregator data processor.

EPCEnricher

A special type of SelectedFieldEnricher that reads an EPC from the user memory of the tag and replaces the manufacturer tag id with the EPC value. Used with non-EPC tags.

EqualizeTimeStamp

Equalizes the time stamp. The time stamp of all RfidEvents is set to the value of the time stamp of the enclosing DataProcessorEvent. This is useful when grouping single events together to simplify processing on the AIN side and when detailed millisecond-level time stamps are not required.

EventTypeFilter

Filters out RFID events based on type. Either "APPEARED" or "DISAPPEARED" events are filtered out.

HierarchyBuilderSend

Builds RFID events into simple hierarchies (for example, the building of a pallet with information about the cases contained on the pallet).

The following assumptions are made:

- We have a simple hierarchy of one single container object (such as a pallet), containing an unlimited number of contained objects (for example, cases).
- Two different readers are used to read the RFID tags of containers and contained objects.
- No new container object appears before the previous one has disappeared (physically impossible for this to happen).
- No contained objects appear if there is no container object. Should this happen, the contained objects are assigned to the next visible container. The error condition is logged.

The building is done according to the following algorithm:

- (Start state) No events have been received.
- When a container "appeared" event is received, the building process starts.
- All following "appeared" events for contained objects are assigned to the current container.
- When a "disappeared" event for the same container is received, the building of the current container is finished. The data is transformed into a message by the assigned transformer object and sent out.

More complex hierarchies, or the association with delivery or order numbers, can only be done at a higher level such as an AutoID Node.

SimplePackSend

This data processor does a simple packing operation assuming a single read point. A read point could be composed of several physical readers, but the algorithm regards them as one.

Like HierarchyBuilderSend, it builds RFID events into simple hierarchies. An example is the building of a pallet with information about the cases contained on the pallet.

The following assumptions are made:

- We have a simple hierarchy of one single container, containing an unlimited number of contained objects.
- The first tag seen is interpreted as the container.
- No new container object appears before the previous one has disappeared (physically impossible for this to happen).
- No contained objects appear if there is no container object. Should this happen, the contained object is interpreted as a container and we cannot recognize this situation as error.

How the building is done depends upon the option setting.

LowPassFilter

Shortly buffers events to filter out false “disappeared” events. This data processor is usually the first one in a chain.

SelectedFieldEnricher

Reads data from selected data fields of the tag and adds this data to the event. It uses the FieldNameMapper to map from logical field names to physical addresses on the tag.

Send

Transforms the internal event data structure and sends the information to registered recipients.

TagBitsFilter

Filters tag events based on the contents of the tag fields. You can specify a bit mask and value used to filter tags. TagBitsFilters can filter on the contents of any tag field defined in the field map including the EPC ID.

TimeFixedSizeAggregator

Aggregates several events into a single one. The aggregation is done during a configurable time interval or up to a configurable maximum number of events, whichever comes first. If no events are received during this interval, no event is forwarded.

About Transformers

The sender type data processors (Send, HierarchyBuilderSend) use a transformer to transform the internal event data structure into a message string and send the message out. The following transformers are available:

EPCPMLTransformer

Specialization of PMLTransformer, where the tag id is given in the EPC URN-notation. The tag IDs should be valid EPCs. Otherwise the numbers are reported as either epc.raw or empty EPCs.

MultiEPCPMLTransformer

Specialization of PMLTransformer, where the tag ID is given both as a hexadecimal string as well as in the EPC URN-notation, separated by a comma. The tag IDs must be valid EPCs. This transformer is mainly used for debugging.

PMLTransformer

Generates a message conforming to the PML Core 1.0 specification. Tag IDs are given as hexadecimal strings.

PMLTransformer2

Specialization of PMLTransformer that does not return a schema ID in XML messages. This creates XML compatible with SAP-AII version 4.0.

PMLTransformerAII4

Specialization of PMLTransformer that populates XML messages with EPC_1.30 schema IDs. This creates XML compatible with SAP-AII version 4.0.

ValidEPCPMLTransformer

Similar to EPCMLTransformer, where the tag IDis given in the EPC URN-notation. Non-valid EPCs are removed from the message and not reported. If no valid tags are in the event structure, no message is sent.

About Data Processor Options

You can set a variety of options for each data processor. One option applies to all processor types, some apply only to sender types, and others are specific to one data processor class.

Options for All Processor Types

These options apply to any data processor type (class: DataProcessor):

ReaderID
The ID of a reader from which RfidEvents are to be received. Used only if the data processor receives events directly from a reader.

Options for Send Processors

These options apply only to send processors (Send, HierarchyBuilderSend):

ReceiverID
The ID of a receiver (AIN) where notifications are sent.

Transformer
The class name of the transformer to be used to transform the internal DataProcessorEvents into a message (for example, into PML Core).

InCommand
The command used in the PML Core message for "appeared" events. Default is null.

OutCommand
The command used in the PML Core message for "disappeared" events. Default is OUT.

Options for CheckReader

CheckParams
The ID of the reader to be checked (optionally, an ID of a check tag). The two values are separated by a comma, as in "ReaderID, CheckTagID". The CheckTagID is a hex string.

TimerInterval
The time (in seconds) between two reader checks. Default is 10.

Options for EPCEnricher

EPCFieldName
The logical field name where the EPC is stored. The mapping table used is defined with the parameter "MappingTable" of the SelectedFieldEnricher. Default is EPC.

Note that all options of the SelectedFieldEnricher are also valid for this data processor.

FilterBadTags
Boolean value indicating if tags where the EPC could not be read should be filtered out (true) or not (false). If set to false, the original tag ID is used as ID for tags that could not be read. Default is false.

Options for EventTypeFilter

FilterAppeared
Boolean value (true/false) indicating if "appeared" events should be filtered out. Default is false.

Filter Disappeared
Boolean value (true/false) indicating if "disappeared" events should be filtered out. Default is true.

Options for HierarchyBuilderSend

ContainedObjectReader
The ID of the reader used for identifying contained objects (such as cases).

ContainerReader
The ID of the reader used for identifying the container object (such as a pallet).

InCommand
The command used to be used in the PML Core message. This is a redefinition of the "InCommand" parameter of the parent SendDataProcessor class. Default is PACK.

Options for SimplePackSend

SendTrigger
Defines when to trigger the sending of the packing message. If set to "Container", the message is sent as soon as the container tag disappears. If set to "All", then the message is sent when no more tags are seen. Default is Container.

RemoveTags
If set to true, tags that disappear are removed from the list (except the pallet). The risk of using this setting is that tags may be reported as “disappeared” due to a misread, although they are still in the field. Default is false.

InCommand
The command used to be used in the PML Core message. This is a redefinition of the the "InCommand" parameter of the parent SendDataProcessor class. Default is PACK.

Options for LowPassFilter

TimerInterval
The time (in milliseconds) to wait before a “disappeared” event is sent on. If an “appeared” event appears within this time interval, no events are sent on. Default is 100.

Options for SelectedFieldEnricher

AddField
Adds the logical field name of a data field that should be read. This option can be repeated multiple times.

ClearFields
Clears the list of data fields that should be read. Not necessary in complete configuration files.

MappingTable
The name of the mapping table for converting logical field names into physical memory addresses on the tag. The mapping tables are defined in the global field map.

RemoveField
Removes a logical field name from the data fields that should be read. This option can be repeated multiple times. Not necessary in complete configuration files.

Retries
The number of read retries performed if there was an error reading a data field.

Options for TagBitsFilter

FilterField

Defines the tag data that will be filtered on. The default value is "EPC", which uses the EPC tag ID. Note that when filtering on fields other than tag ID, the data must already be in the event passed on to this data processor. Thus, you must place a SelectedFieldEnricher data processor in your pipeline in front of this data processor to filter on user data fields.

FilterBitMask

Defines the bit comparison you want to make on the tag field. 1s and 0s indicate mandatory bit values. Xs mean "don't care". If the mask is smaller than the actual data, the extra data is not checked. If the mask is longer than the tag data, the tag event fails the comparison.

The mask can be specified in base-2 or in hexadecimal (prepend an H). For example, the filter mask `00110000XXXX00101111` can also be expressed as `H30x2F`.

Invert

A Boolean value that defines the filter effect. If false (default), only tag events that pass the bit filter are passed on in the pipeline. If true, only tag events that fail the bit filter are passed on in the pipeline.

Here is example XML showing use of the filter options:

```
<DataProcessor id="tfilter" description="TagIDFilter">
   <APIImplementationClass>
      com.sap.devicecontroller.core.dataprocessors.TagBitsFilter
   </APIImplementationClass>
   <OptionList>
      <opt:FilterBitMask>00110000XXXX0010</opt:FilterBitMask>
      <opt:Invert>false</opt:Invert>
   </OptionList>
</DataProcessor>
```

Options for TimeFixedSizeAggregator

MaxCount

The maximum number of events for the aggregation. All events are counted until this number is reached or until the maximum time interval since the first event has passed. Aggregated events within the message keep their original timestamp. Default is 100.

TimerInterval

The length of the time window (in milliseconds) for the aggregation. All events within this window are aggregated into a single message, unless the maximum number of events is reached first. Aggregated events within the message keep their original timestamp. Default is 10000.

Index

Symbols
$JAVA_HOME, described, **69**
$JDBC_HOME, described, **69**
/cf/startup, **43**
/home/developer/startup, **43**

Numerics
802.11g radio
  advanced parameters, setting, **39**
  Antenna Control, **41**
  antenna guidelines, **26**
  antenna port locations, **8**
  Client Type/Performance, **40**
  configuring, **37**
  connection, configuring, **15**
  Enable CCxv2 Radio Measurements, **41**
  Enable CCxv2 Rogue Detection, **41**
  Enable Medium Reservation, **40**
  Fragmentation Threshold, **40**
  IF5 in wireless network, illustrated, **9**
  network, illustrated, **9**
  Power Output Level, **40**
  screen, illustrated, **37**
  settings, described, **38**
  specifications, **135**
  troubleshooting problems, **120**
802.1x client settings, described, **60**

A
About This IF5 RFID Reader screen, **114**
AC power port
  described, **5**
  location, **4**
access point MAC address, viewing, **110**
access point neighbors, viewing in Maintenance menu, **111**
access via menus, controlling, **42**
AddField option, for SAP data processors, **162**
Address field, in AP Neighbors screen, **112**
advanced parameters, for 802.11g radio, **39**
Age field, in AP Neighbors screen, **112**
Allow External BRI Connection setting, **81**
Allow External EPC Connection setting, **81**
Allow External EPC Connections check box, **81**
Allow ICMP Configuration check box, **43**
Allow LEAP check box, **60**
Allow PEAP check box, **60**
Allow Service Password check box, **49**
Allow Telnet Shell Access check box, **45**
Allow TLS check box, **60**
Allow TTLS (MSCHAPv2) check box, **60**
Always Use DHCP setting, **32**
Antenna Control setting, for 802.11g radio, **41**
antenna firing sequence, for RFID, described, **79**
antenna placement, for 802.11g radio, **26**
Antenna Timeout setting, 77
Antenna Tries setting, 77
ANTTIMEOUT equivalent, 77
ANTTRIES equivalent, 77
AP Neighbors screen
  described and illustrated, **111**
  fields, described, **112**
applications
  command line arguments, handling at boot time, **71**
  configuring data collection engine, **80**
  developing with Workbench tool, **91**
  how to develop, **67**
  IF5 RFID architecture, illustrated, **73**
  Java support, **68**
  Java, executing on IF5, **68**
  JavaScript support, **70**
  starting at boot time, **70**
  using with IF5, **66**
Apply Hot Settings, **40**
Authentication Method setting
  dynamic WEP, **54**
  WPA2-802.1x, **60**
  WPA-802.1x, **56**
Authentication Protocol setting, SNMPv3, **100**
Automount NFS check box, **45**
auto-run file
  applications, running at boot time, **43**
  at boot time, **92**
  configuring with JavaScript tool, **92**
  scripts, running at boot time, **43**

auto-starting applications at boot time, 70
Avalanche. *See* Wavelink Avalanche

B

Basic Reader Interface
  attribute equivalents for RFID module settings, 75
  external connections, enabling, 81
  Heartbeat setting, 81
  in IF5 RFID architecture, 73
  script files, loading and running with Diagnostics tool, 87
  sending commands with Diagnostics tool, 84, 87
  TCP Port setting, for DCE, 81
  used in IF5 RFID architecture, illustrated, 73
  window, in Diagnostics tool, 87
blue LED, described, 7
booting the IF5
  applications, starting at boot time, 70
  auto-running JavaScript, 92
bracket, mounting, described, 24
BRI Commands screen, illustrated, 87
BRI Heartbeat setting, 81
BRI TCP Port setting, for DCE, 81
BRI. *See* Basic Reader Interface
Browser Access setting, described, 43

C

cable access door, removing, 4
Capabilities field, in AP Neighbors screen, 112
cautions, described, xiii
CDC/Foundation profile, 68
Certificate Details screen, illustrated, 62
Certificate Import screen, illustrated, 63
certificates
  described, 61
  expired, rejecting, 64
  installing and uninstalling, 62
  viewing, 61
changes, saving, 22
Channel field, in AP Neighbors screen, 112
CheckParams option, for SAP data processors, 160
CheckReader, 156
  options, 160
ClearFields option, for SAP data processors, 162
Client Type/Performance setting, for 802.11g radio, 40
command line arguments, handling at boot time, 71
configuring the IF5
  802.11g radio settings, 37
  active configuration file, described, 22
  applications, starting at boot time, 70
  connecting via 802.11g radio, 15
  connecting via Ethernet, 13
  connecting with communications program, 10
  current configuration file, described, 22
  data collection engine, 80
  default configuration file, described, 22
  default configuration, restoring, 118
  DHCP settings
    802.11g radio, 37
    Ethernet, 32
  DNS settings, 34
  Ethernet link speed, 30
  Ethernet settings, 30
  firmware, upgrading, 123
  Intermec Settings, using, 103
  IP address, 10
  network services, 34
  network settings, 30
  password server, 46
  RFID settings, 74
  saving changes, 22
  security, 41
  setting IP address, described, 10
  SNTP client settings, 36
  summary of configuration settings in Maintenance menu, 116
  summary of settings, viewing, 116
  SYSLOG destination, 34
  user name and password, setting, 45
  using web browser interface, 19
  viewing summary, 114
connecting IF5 to network, 25
ContainedObjectReader option, for SAP data processors, 161

ContainerReader option, for SAP data processors, 161
control port
location, 4
pin assignments, 137
Controller ID element, 144
controlling access to IF5 menus, 42

D

data collection engine
Allow External BRI Connection, 81
Allow External EPC Connection, 81
BRI Heartbeat, 81
BRI TCP Port, 81
configuring, 80
Enable Logging, 81
EPC TCP Port, 81
log, enabling and viewing, 82
logfile command event descriptions, 83
settings, described, 81
statistics, viewing, 83
trigger, managing, 81
using with Intermec Ready-To-Work indicator, 7
Data Privacy Protocol setting, for SNMPv3, 100
data processors, for SAP device controller, 152
standard, list of, 156
date and time
setting with web browser interface, 27
SNTP client settings, 36
DCE Configuration screen, illustrated, 80
DCE. *See* data collection engine
default configuration, restoring, 118
default login, changing, 48
defaults, restoring, 118
developer tools
described, 71
enabling, 72
developing applications
access, controlling, 44
auto-running JavaScript files at boot time, 92
command line arguments at boot time, 71
edgeware, defined, 71
fine-tuning with Diagnostics tool, 84
guidelines, 67
IF5 RFID architecture, illustrated, 73
Java support, 68
JavaScript support, 70
JavaScript tool, 90
shell script, example, 71
SQL server support, 69
starting at boot time, 70
using with IF5, 66
with Intermec RFID Resource Kit, 67
device controller. *See* SAP device controller
DHCP Mode setting, 32
DHCP settings, configuring
802.11g radio, 37
Ethernet, 32
diagnostics
access point connections, viewing, 110
access point neighbors, viewing, 111
configuration summary, viewing, 114
data collection engine events log, viewing, 82
data collection engine statistics, viewing, 83
events log, viewing, 113
port statistics, viewing, 113
Diagnostics tool, 84
BRI window, 87
GPIO, testing, 86
tags, reading and displaying IDs, 85
Disable DHCP setting, 32
Display Log screen, for DCE, illustrated, 82
Display Tags screen, illustrated, 85
DNS settings, configuring, 34
DuplicateFilter, 156
dynamic WEP
802.1x client settings, 60
configuring, 52

E

edgeware
advantages, 66
defined, 66
developer tools, described, 71
SAP device controller, enabling, 72
electrical specifications, 134

Enable Antenna Port check box, 79
Enable Autoconfiguration, for IPv6, 33
Enable CCKM check box, 56
Enable CCxv2 Radio Measurements, 41
Enable CCxv2 Rogue Detection, 41
Enable FTP Server check box, 45
Enable Logging check box, for DCE, 81
Enable Medium Reservation check box, 40
Enable mixed cell check box
  dynamic WEP, 54
  static WEP, 52
Enable Startup Scripts check box, 43
EPC TCP Port setting, 81
EPCEnricher, 156
  options, 161
EPCFieldReader option, for SAP data processors, 161
EPCglobal Class 1 Gen 2
  certification, 3
  tags, choosing in RFID Module settings, 75
EPCPML transformer, 159
EqualizeTimeStamp, 157
Ethernet
  connection, configuring, 13
  IF5 in wired network, illustrated, 9
  link speed, configuring, 30
  port
    described, 5
    pin assignments, 138
  settings
    configuring with web browser interface, 30
    described, 32
  troubleshooting problems, 120
Ethernet port
  location, 4
Events Log screen, illustrated, 114
events log, viewing in Maintenance menu, 113
EventTypeFilter, 157
  options, 161
exporting files, 104
ExtensionCommandHandler, 146
external controls, using with IF5, 126

F

features, new in this release, 2
Field Separator setting, 76
Field Strength setting, 79
FieldMap.xml, described, 143
fields, in tags, separating, 76
FIELDSEP equivalent, 76
FIELDSTRENGTH equivalent, 79
File Import and Export screen, illustrated, 105
File System Directory screen, illustrated, 105
files, importing and exporting, 104
  troubleshooting, 122
  using web browser, 104
  with FTP server, 108
FilterAppeared option, for SAP data processors, 161
FilterBadTags option, for SAP data processors, 161
FilterBitMask option, for SAP data processors, 163
FilterDisappeared option, for SAP data processors, 161
FilterField option, for SAP data processors, 163
firmware upgrades, 123
Fragmentation Threshold setting, for 802.11g radio, 40
front panel ports
  accessing, 4
  described, 5
FTP server
  access, enabling or disabling, 44
  allowing access, 45
  default login and password, 45
  importing and exporting files, 108

G

general purpose input/output interfaces
  accessing, 126
  described, 126
  Diagnostics tool, testing with, 86
  inputs, using, 127
  isolated input, 128
  open collector input, 128

general purpose input/output interfaces (*continued*)
output, switching high side using external power, **131**
output, switching the high side, **130**
output, switching the low side, **130**
outputs, using, **129**
power, using, **132**
powered input, **127**
relay, driving to control AC load, **131**
WRITEGPIO equivalents, **86**
GPIO. *See* general purpose input/output interfaces

H

HierarchyBuilderSend, **157**
options, **161**
hot settings, defined, **40**
HyperTerminal, using to configure IF5, **10**

I

IBM
Services Management Framework (SMF), **68**
WebSphere Everyplace MicroEnvironment (WEME), **68**
ICMP access, enabling or disabling, **42**
ID Report check box, **76**
ID Timeout setting, 77
ID Tries setting, 77
IDREPORT equivalent, **76**
IDTIMEOUT equivalent, 77
IDTRIES equivalent, 77
IF5
802.11g network, described and illustrated, **9**
applications, developing, **67**
applications, starting at boot time, **70**
configuration summary, viewing, **116**
connecting to network, **25**
connecting with communications program, **10**
default configuration, restoring, **118**
described, **2**
developer access, controlling, **44**
DHCP state, described, **10**
dimensions, **134**
environmental requirements, **24**
Ethernet network, described and illustrated, **9**
files, importing and exporting, **104**
using web browser, **104**
with FTP server, **108**
firmware, upgrading, **123**
installing, **24**
IP address, setting, **10**
Java support, **68**
JavaScript support, **70**
learning about, **4**
locating with LEDs, **115**
maintaining, **110**
managing, **98**
mounting location, choosing, **24**
overview, **2**
related documents, list of, **xv**
requirements, environmental, **24**
RFID architecture, illustrated, **73**
RFID settings, configuring, **74**
SAP device controller, enabling, **72**
SNMP, managing with, **98**
specifications, **134**
troubleshooting, **119**
unpacking, **3**
using securely, **28**
what's new in this release, **2**
Wi-Fi certification, **3**
WRDI, enabling, **72**
importing files, **104**
InCommand option, for SAP data processors, **161**, **162**
InCommand transformer, for SAP data processors, **160**
indicator lamps
testing with IF5, **86**
using with IF5, **126**
Init Tries setting, **78**
Initial Queue setting, **79**
initialize tags setting, **78**
INITIALQ equivalent, **79**
INITTRIES equivalent, **78**

input interface
isolated, 128
open collector, 128
powered, 127
signal descriptions, 127
installing
802.11g antennas, 25
IF5, 24
RFID antennas, 25
Intermec
Global Sales and Service, xiii
Knowledge Central, xiii
manuals, how to download from web, xv
Product Support, what to know when calling, 122
Settings, application, 103
SmartSystems Console, 103
Internet Protocol version 6
enabling in communications program, 17
enabling in web browser interface, 33
Invert option, for SAP data processors, 163
IP address, setting, 10
saving changes, 22
with communications program, 10
with web browser interface, 30
IPv6. *See* Internet Protocol version 6

J

J2ME support, 68
J2SE support, 68
j9 on IF5, described, 69
Java programming
$JAVA_HOME, 69
$JDBC_HOME, 69
IF5 support, 68
j9, 69
jar files, running, 68
jcl:foun10, 69
JIT compiler, enabling, 69
libraries, described, 68
running applications on IF5, 68
SQL server support, 69
JavaScript
Auto Start screen, illustrated, 94
files, importing and running, 91
support, 70
JavaScript tool
described, 90
remote startup files, editing, 94
running a file at boot time, 92
Workbench, using to test scripts, 91
jcl:foun10, described, 69

L

LEDs
described, 6
Intermec Ready-To-Work Indicator, 6
location, 6
power, 6
using to locate the IF5, 115
wired LAN, 6
wireless, 6
location, choosing for IF5, 24
Lock Tries setting, 78
LOCKTRIES equivalent, 78
login screen, 19
login, changing default, 48
LowPassFilter, 158
options, 162

M

MAC address of current access point, viewing in Maintenance menu, 110
maintaining the IF5, 110
Maintenance menu, 110
About This IF5 RFID Reader screen, 114
access point neighbors, viewing, 111
configuration summary, 116
connections, viewing, 110
events log, viewing, 113
locating the IF5, 115
port statistics, viewing, 113
using LEDs to locate the IF5, 115
managing the IF5
access to configuration menus, controlling, 42
defaults, restoring, 118
developer access, controlling, 44
firmware, upgrading, 123
methods, 98
security, configuring, 41

managing the IF5 (*continued*)
SmartSystems Console, **103**
SNMP, **98**
using securely, **28**
manuals, Intermec, how to download from web, **xv**
MappingTable option, for SAP data processors, **162**
MaxCount option, for SAP data processors, **163**
menu access, controlling, **42**
Minimum Multicast Encryption Type
WPA2-802.1x, **60**
WPA2-PSK, described, **58**
WPA-802.1x, **56**
motion sensors
testing with IF5, **86**
using with IF5, **126**
mounting location, choosing, **24**
MultiEPCPML transformer, **159**

N

network
802.11g connection, in communications program, **15**
connecting IF5 to, **25**
Ethernet connection, in communications program, **13**
IF5 illustrated in, **9**
network services
DNS settings, configuring, **34**
SNTP client settings, configuring, **36**
SYSLOG destination, configuring, **34**
NFS
Automount NFS settings, described, **45**
shared drive, enabling or disabling, **44**
No Tag Report check box, **76**
NOTAGRPT equivalent, **76**
NOTAGS message, enabling or disabling, **76**
notes, described, **xiii**

O

OSGi support, **68**
OutCommand option, for SAP data processors, **160**
output interface
driving external DC relay, **131**
high side switching, **130**
high side switching with external power, **131**
low side switching, **130**
signal descriptions, **129**
output interfaces, **129**
overview of the IF5, **2**

P

Password
802.1x client, **61**
user login, **49**
password settings, described, **49**
Passwords screen, illustrated, **46**
patent information, **xvi**
Performance screen, illustrated, **89**
pin assignments, for ports, **137**
pinouts, **137**
PMLTransformer, **159**
PMLTransformer2, **159**
PMLTransformerAII4, **159**
port pin assignments
control, **137**
Ethernet, **138**
serial, **138**
Port Statistics screen, illustrated, **113**
port statistics, viewing in Maintenance menu, **113**
ports
802.11g radio antenna, **8**
AC power, **5**
control, **5**
Ethernet, **5**
front panel, accessing, **4**
front panel, described, **5**
pin assignments, **137**
rear panel, described, **8**
RFID antenna, **8**
serial, **5**
power interface, **132**
Power Output Level setting, for 802.11g radio, **40**
power port, described, **5**
Preferred Protocol setting, 802.1x client, **61**
Pre-Shared Key, for WPA2-PSK, **58**

problems with IF5, solving, **119**
ProcessChainList, **146**
Product Support, calling Intermec, **122**
proxy server, using to access Internet, **19**

R

radio. *See* 802.11g radio
RADIUS authentication server, described, **45**
RDTRIES equivalent, **78**
Read Only Password setting, **49**
Read Tries setting, **78**
Reader List, **146**
reader module, settings, **74**
ReaderID, for SAP device controller, **160**
Ready-to-Work indicator, described, **7**
rear panel ports, described and illustrated, **8**
ReceiverID option, for SAP data processors, **160**
ReceiverList, **145**
Reject Expired Certificates check box, **43**, **64**
RemoveField option, for SAP data processors, **162**
RemoveTags option, for SAP data processors, **162**
Retries option, for SAP data processors, **162**
RFID
  antenna firing sequence, described, **79**
  antenna port locations, **8**
  applications, using with IF5, **66**
  architecture, illustrated, **73**
  Diagnostics tool, using to test system, **84**
  edgeware, enabling, **72**
  IF5 settings, described, **75**
  Java support, **68**
  JavaScript support, **70**
  module, configuring, **74**
  Resource Kit, described, **67**
  SAP device controller, using, **140**
  specifications, **136**
  tags, reading and displaying with Diagnostics tool, **85**
  troubleshooting problems, **119**
RFID Edgeware screen, illustrated, **72**
RFID Module screen, illustrated, **74**
RfidReader.properties
  elements, defined, **148**
  file, described, **143**, **148**
running Java applications on IF5, **68**

S

safety information, **xiii**
SAP device controller, **140**
  changing settings in configuration files, **144**
  configuration file generator, using, **142**
  configuration files, described, **143**
  configuring, **140**
  Controller ID, **144**
  data processors
    AddField option for SelectedFieldEnricher, **162**
    CheckParams option for CheckReader, **160**
    CheckReader, **156**
    ClearFields option for SelectedFieldEnricher, **162**
    ContainedObjectReader option for HierarchyBuilderSend, **161**
    ContainerReader option for HierarchyBuilderSend, **161**
    described, **152**
    DuplicateFilter, **156**
    EPCEnricher, **156**
    EPCFieldName option for EPCEnricher, **161**
    EqualizeTimeStamp, **157**
    EventTypeFilter, **157**
    FilterAppeared option for EventTypeFilter, **161**
    FilterBadTags option for EPCEnricher, **161**
    FilterBitMask option for TagBitsFilter, **163**
    FilterDisappeared option for EventTypeFilter, **161**
    FilterField option for TagBitsFilter, **163**
    HierarchyBuilderSend, **157**
    illustrated, **153**

SAP device controller: data processors (*continued*)
InCommand option for HierarchyBuilderSend, **161**
InCommand option for send processors, **160**
InCommand option for SimplePackSend, **162**
Invert option for TagBitsFilter, **163**
LowPassFilter, **158**
MappingTable option for SelectedFieldEnricher, **162**
MaxCount option for TimeFixedSizeAggregator, **163**
nonlinear, illustrated, **155**
options, **160**
OutCommand option for send processors, **160**
ReaderID option, **160**
Receiver ID option, **160**
RemoveField option for SelectedFieldEnricher, **162**
RemoveTags option for SimplePackSend, **162**
Retries option for SelectedFieldEnricher, **162**
SelectedFieldEnricher, **158**
Send, **158**
SendTrigger option for SimplePackSend, **161**
SimpleDuplicateFilter, **156**
SimplePackSend, **158**
standard, list of, **156**
TagBitsFilter, **158**
TimeFixedSizeAggregator, **159**
TimerInterval option for CheckReader, **160**
TimerInterval option for LowPassFilter, **162**
TimerInterval option for TimeFixedSizeAggregator, **164**
Transformer option, **160**
types, **154**
enabling, **72**
ExtensionCommandHandler, **146**
FieldMap, **146**
logging, **151**
ProcessChainList, **146**
Reader List, **146**
ReceiverList, **145**
reconfiguring manually via Telnet, **141**
reconfiguring via XML commands, **142**
running manually via Telnet, **140**
stopping via XML commands, **142**
transformers, **159**
EPCPML, **159**
MultiEPCPML, **159**
PMLTransformer, **159**
PMLTransformer2, **159**
PMLTransformerAII4, **159**
ValidEPCPML, **159**
SDCConfiguration.xml, described, **143**, **144**
secure web browser interface, using, **19**
securely using the IF5, **28**
security
802.1x client settings, described, **60**
certificates, described, **61**
configuring, **41**
controlling menu access, **42**
default login, changing, **48**
developer access, controlling, **44**
dynamic WEP, **52**
password server, using with IF5, **46**
static WEP, configuring, **50**
supported methods, **41**
WPA2-802.1x, **58**
WPA2-PSK, **57**
WPA-802.1x, **55**
WPA-PSK, **54**
SelectedFieldEnricher, **158**
options, **162**
Send, **158**
SendTrigger option, for SAP data processors, **161**
serial port
location, **4**
pin assignments, **138**
service password, described, **49**
SESSION equivalent, **79**
Session setting, **79**
Set Clock screen, **27**

shell script, example, 71
Signal (dBm) field, in AP Neighbors screen, 112
Simple Network Time Protocol (SNTP) client settings, configuring, 36
SimpleDevice.property file, described, 143
SimpleDuplicateFilter, 156
SimplePackSend, 158
  options, 161
SmartSystems Console, Intermec, using to manage IF5, 103
SNMP
  Community settings, described, 100
  parameters, described, 100
  using to manage IF5, 98
SNMPv3
  Authentication Protocol, 100
  Data Privacy Protocol, 100
  enabling, 98
  settings, described, 100
specifications
  802.11g radio, 135
  electrical and physical, 134
  RFID, 136
SQL server, driver for IF5, 68
SSID field, in AP Neighbors screen, 112
startup file
  configuring JavaScript, 92
  editing, 94
  uploading from PC, 94
support, calling Intermec, 122
SYSLOG destination
  configuring, 34
  defined, 35
SYSLOG server, 35

T

Tag Type setting, 75
TagBitsFilter, 158
  options, 163
tags, RFID
  choosing type, 75
  ID reporting, enabling or disabling, 76
  read performance
    described, 90
  reading with Diagnostics tool, 85
TAGTYPE equivalent, 75
TCP/IP screen, illustrated, 31
TCP/IP settings, configuring, 30
Telnet
  access, enabling or disabling, 44
  allowing shell access, 45
  connecting to the IF5, 141
  default login and password, 45
terminators, location, 8
time and date
  setting with web browser interface, 27
  SNTP client settings, 36
TimeFixedSizeAggregator, 159
  options, 163
Timeout Configuration mode, enabling, 76
TIMEOUTMODE equivalent, 76
TimerInterval option, for SAP data processors, 160, 162, 164
TKIP (RSN), 56, 58
tools
  Developer, described, 71
  Diagnostics, 84
  JavaScript, 90
Transformer option, for SAP data processors, 160
transformers, for SAP device controller, 159
trigger, managing with data collection engine, 81
TRIGGERREADY command, from DCE, 81
troubleshooting the IF5, 119
  access point neighbors, viewing in Maintenance menu, 111
  connectivity problems, 120
  default configuration, restoring, 118
  Intermec Product Support, calling, 122
  MAC address of current access point, viewing, 110
  Maintenance menu, viewing, 110
  port statistics, viewing, 113
  problems copying files, 122
  RFID problems, 119

U

unpacking the IF5, 3
upgrade files, where to find, 123

Upgrade Software screen, illustrated, **123**
upgrading firmware, **123**
Use DHCP if IP Address is Zero setting, **32**
Use RADIUS for Login Authorization check box, **49**
user class, DHCP, described, **38**
User Name setting, 802.1x client, **61**
User Name setting, for passwords, **49**

V

ValidEPCPML transformer, **159**
vendor class, DHCP, described, **39**
Verify CA Certificate setting, 802.1x client, **61**

W

warnings, described, **xiii**
warranty information, **xiii**
Wavelink Avalanche
  parameters, described, **102**
  using to manage IF5, **101**
web browser interface, **19**
  data collection engine, changing settings, **80**
  date and time, setting, **27**
  defaults, restoring, **118**
  Diagnostics tool, **84**
  enabling or disabling, **42**
  firmware, upgrading, **123**
  importing and exporting files, **104**
  JavaScript tool, **90**
  Maintenance menu, **110**
  RFID edgeware, enabling, **72**
  RFID module, changing settings, **74**
  secure, **20**
  SNMP, enabling, **98**
  Wavelink Avalanche, enabling, **101**
WebSphere Everyplace MicroEnvironment, **68**
WEME. *See* WebSphere Everyplace MicroEnvironment
WEP
  dynamic, configuring, **52**
  dynamic, parameters described, **54**
  key formats for static WEP, described, **52**
  static, configuring, **50**
  static, parameters described, **52**
WEP (TSN), **58**
WEP Method setting, **52**
WEP Transmit Key setting, **52**
what's new in this release, **2**
Wi-Fi certification, for IF5, **3**
Workbench, in JavaScript tool, **91**
WPA2-802.1x security
  Authentication Method, **60**
  configuring, **58**
  Minimum Multicast Encryption Type, **60**
  Network EAP, described, **60**
  Open System, described, **60**
  TKIP (RSN), **60**
  WEP (TSN), **60**
WPA2-PSK security
  configuring, **57**
  Minimum Multicast Encryption Type, **58**
  pre-shared key, **58**
WPA-802.1x security
  802.1x client settings, **60**
  Authentication Method, **56**, **60**
  configuring, **55**
  Enable CCKM, **56**
  Minimum Multicast Encryption Type, **56**
  Network EAP, described, **56**
  Open System, described, **56**
  parameters, described, **56**, **60**
  TKIP (RSN), **56**
  WEP (TSN), **56**
WPA-PSK security
  configuring, **54**
  pre-shared key, **55**
WRDI option
  described, **66**
  enabling, **72**
  SuperFeature CD, described, **67**
Write Tries setting, **78**
WRTRIES equivalent, **78**